



Report di applicazione Web

Questo report include importanti informazioni di sicurezza sull'applicazione Web.

Report Sicurezza

Questo report è stato creato da IBM Security AppScan Standard 9.0.3.12 iFix002, Regole: 17441
Scansione avviata: 27/01/2020 17:20:35

Sommario

Introduzione

- Informazioni generali
- Impostazioni di login

Riepilogo

- Tipi di problemi
- URL vulnerabili
- Raccomandazioni fix
- Rischi di sicurezza
- Cause
- Classificazione minaccia WASC

Problemi ordinati per tipo di problema

- Manca un attributo sicuro nella sessione cookie crittografata (SSL) ⑤
- Intestazione "Content-Security-Policy" mancante o non sicura ④
- Intestazione "X-Content-Type-Options" mancante o non sicura ④
- Intestazione "X-XSS-Protection" mancante o non sicura ④
- Intestazione HSTS (HTTP Strict-Transport-Security) mancante o non sicura ④
- Manca l'attributo HttpOnly nel cookie di sessione ②
- Difesa scripting tra frame mancante o non sicura - Estesa e informativa ②
- Individuazione di possibile pattern di divulgazione percorso server ②
- Riferimenti cookie (JavaScript) lato client ①

Dati di applicazione

- Parametri
- URL visitati

Introduzione

Questo report contiene i risultati di una scansione di sicurezza dell'applicazione Web eseguita da IBM Security AppScan Standard.

Problemi di severità media:	5
Problemi di severità bassa:	18
Problemi di severità informazioni:	5
Problemi di sicurezza totali inclusi nel report:	28
Problemi di sicurezza totali rilevati nella scansione:	28

Informazioni generali

Nome file di scansione: conam

Scansione avviata: 27/01/2020 17:20:35

Polizza del test: Completo

Host tst-secure.sistemapiemonte.it

Porta 443

Sistema operativo: Unix

Server Web: Oracle Web Listener

Server di applicazioni: JavaAppServer

Impostazioni di login

Metodo di login: Login registrato

Login simultanei: Abilitato

Esecuzione JavaScript: Abilitato

Rilevamento in-session: Abilitato

Pattern in-session: meta\ name|/conam/main\.bundle\.js

Cookie ID sessione o tracciati: JSESSIONID
_idp_authn_lc_key
_idp_session
_shibsession_spsliv1SISP
JSESSIONID
XSRF-TOKEN

Parametri ID sessione o tracciati: SAMLRequest
RelayState
RelayState
SAMLResponse

Sequenza di login:

```
https://tst-secure.sistemapiemonte.it/conam
https://tst-
secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTLjpswFibX06dA3ofblExiJZFSglSkXCgwUdVNZMxJYwlsapuZzNvX
5KJG6UxUzaJqvUHgc/nOf34xUqSuGjxt9Y6n8KMFpa19XXGFDxdj1EqOBVEMYU5qUFhT
nE0Xc+zbLm6k0IKKC1lTpUBqJngouGprkBnIJ0bhMZ2P0U7rRmHH0Ur3FNBWgm3qaahJ
w6AWXIPNtFOxJ8/JdqwoRAV6ZyslnK6T7ySrLEfWzKAxTromflqSkZqVjWocA7plFZzq
pVAyCVQ7WbZCVjwbo81g0Pfu/QAe+oOigD4NPOr1iy0JBsOPwyIITJhSLcRcacL1Gpmu
7/Zcr+c/5F4f+/fY9b8hKznp8YnxkvHvt8UrjkEKf87zpHeccQ1SHeYzAWjywy7X2fU
bQQfO0TFjm53IefFoE...
https://tst-secure.sistemapiemonte.it/iamidpsp/AuthnEngine
https://tst-secure.sistemapiemonte.it/iamidpsp/login.jsp?
actionUrl=/iamidpsp/AuthnEngine
https://tst-secure.sistemapiemonte.it/iamidpsp/Authn/X509/Login
https://tst-
secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO
https://tst-secure.sistemapiemonte.it/liv1/Shibboleth.sso/SAML2/POST
https://tst-secure.sistemapiemonte.it/conam
https://tst-secure.sistemapiemonte.it/conam/
https://tst-
secure.sistemapiemonte.it/conam/restfacade/user/getProfilo
```

Riepilogo

Tipi di problemi 9

[Sommar](#)

Tipo di problema		Numero di problemi	
M	Manca un attributo sicuro nella sessione cookie crittografata (SSL)	5	<div><div></div></div>
B	Intestazione "Content-Security-Policy" mancante o non sicura	4	<div><div></div></div>
B	Intestazione "X-Content-Type-Options" mancante o non sicura	4	<div><div></div></div>
B	Intestazione "X-XSS-Protection" mancante o non sicura	4	<div><div></div></div>
B	Intestazione HSTS (HTTP Strict-Transport-Security) mancante o non sicura	4	<div><div></div></div>
B	Manca l'attributo HttpOnly nel cookie di sessione	2	<div><div></div></div>
I	Difesa scripting tra frame mancante o non sicura - Estesa e informativa	2	<div><div></div></div>
I	Individuazione di possibile pattern di divulgazione percorso server	2	<div><div></div></div>
I	Riferimenti cookie (JavaScript) lato client	1	<div><div></div></div>










URL vulnerabili 7

[Sommar](#)

URL		Numero di problemi	
M	https://tst-secure.sistemapiemonte.it/conam	7	<div><div></div></div>
M	https://tst-secure.sistemapiemonte.it/conam/	6	<div><div></div></div>
B	https://tst-secure.sistemapiemonte.it/conam/inline.bundle.js	4	<div><div></div></div>
B	https://tst-secure.sistemapiemonte.it/conam/polyfills.bundle.js	4	<div><div></div></div>
B	https://tst-secure.sistemapiemonte.it/conam/styles.bundle.js	5	<div><div></div></div>
I	https://tst-secure.sistemapiemonte.it/conam/scripts.bundle.js	1	<div><div></div></div>
I	https://tst-secure.sistemapiemonte.it/conam/vendor.bundle.js	1	<div><div></div></div>







Raccomandazioni fix 9

[Sommar](#)

Operazione di risoluzione		Numero di problemi	
M	Aggiungere l'attributo 'Secure' a tutti i cookie sensibili	5	
B	Aggiungere l'attributo 'HttpOnly' a tutti i cookie di sessione	2	
B	Configurare il server per l'utilizzo dell'intestazione "Content-Security-Policy" con politiche sicure	4	
B	Configurare il server per l'utilizzo dell'intestazione "X-Content-Type-Options" con il valore "nosniff"	4	
B	Configurare il server per l'utilizzo dell'intestazione "X-Frame-Options" con il valore DENY o SAMEORIGIN	2	
B	Configurare il server per l'utilizzo dell'intestazione "X-XSS-Protection" con il valore '1' (abilitato)	4	
B	Implementare la politica HSTS (HTTP Strict-Transport-Security) con un valore esteso di "max-age"	4	
B	Rimuovere la logica di business e di sicurezza dal lato client	1	
B	Scaricare la patch di sicurezza pertinente per il server Web o l'applicazione Web.	2	

Rischi di sicurezza 6







[Sommar](#)

Rischio		Numero di problemi	
M	È possibile intercettare le informazioni relative all'utente e alla sessione (i cookie), inviate durante una sessione crittografata	5	
B	È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili	18	
B	È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.	18	
B	È possibile che la sessione del cliente e i cookie vengano intercettati o manipolati e potrebbero essere utilizzati per impersonare un utente legittimo, consentendo così all'aggressore di visualizzare o modificare i record dell'utente e di eseguire transazioni come se fosse tale utente.	2	
I	È possibile richiamare il percorso assoluto di installazione del server Web, che potrebbe essere utile ad un aggressore per sviluppare altri attacchi ed ottenere informazioni sulla struttura del file system dell'applicazione Web	2	
I	Lo scenario di ipotesi peggiore per questo attacco dipende dal contesto e dal ruolo dei cookie creati sul lato client	1	

Cause 6

[Sommar](#)

Causa	Numero di problemi
-------	--------------------

M	L'applicazione Web invia cookie non sicuri su SSL	5	
B	Programmazione o configurazione non sicura dell'applicazione Web	16	
B	L'applicazione Web imposta i cookie di sessione senza l'attributo HttpOnly	2	
I	Insecure web application programming or configuration	2	
I	Non sono state installate le patch o gli hotfix più recenti per i prodotti di terze parti.	2	
I	I cookie vengono creati sul lato client	1	

Classificazione minaccia WASC

[Sommar](#)

Minaccia	Numero di problemi	
Perdita di informazioni	28	

Problemi ordinati per tipo di problema

M Manca un attributo sicuro nella sessione cookie crittografata (SSL) 5 Sommario

Problema 1 di 5

Sommario

Manca un attributo sicuro nella sessione cookie crittografata (SSL)

Severità:	Media
Punteggio CVSS:	6,4
URL:	https://tst-secure.sistemapiemonte.it/conam
Entità:	_shibstate_793b2168 (Cookie)
Rischio:	È possibile intercettare le informazioni relative all'utente e alla sessione (i cookie), inviate durante una sessione crittografata
Cause:	L'applicazione Web invia cookie non sicuri su SSL
Fix:	Aggiungere l'attributo 'Secure' a tutti i cookie sensibili

Differenza:

Motivazione: AppScan ha rilevato che una sessione crittografata (SSL) sta utilizzando un cookie senza l'attributo "secure".

Richieste e risposte del test:

```
GET /conam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: __utma=32890173.1526803074.1567412775.1567412775.1567412775.1;
__utms=32890173.1567412775.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
```



```

SAMLRequest=1ZTLjpswFIbX06dA3odbBqaxkkkgpQSpSLhSYqOomcvBJYwlsapuZzNvX5KJGmWlUzaJqvUHgc%2FnOf34xVKS
uGjxp9Y5n8KMFpa19XXGFDxcj1EqOBVfMYU5qUFIxOJ%2FMZ9i3XdxIoUUpKmRNlAKpmeCR4KqtQeYgnlgJj9lshHZAwo7j1
a6p6BsJdimnoaaNaxqWTXTDsVe%2FKcfMc2G1GB3t1KCafr5DvpMi%2BQNTVojJouyZ%2BWZKRmtFGNY0C3rIJTvQwok1BqJ
8%2BXyEqmI7Qow4DQ%2Fkca%2Bpsw9PsPQq1Bf7sNHwaBR6nbN2FKtZBwpQnXI%2BS7vttzv7fLbx7fO%2FiYPANWelJj0%2
BMU8a%2F3xZvcwXs%2BHNRpL3jjCuQ6jCfCUDjD%2Bbc%2FTrDbiP4wCEvdnS7CzkvBo3zOfs1UbxOs%2BUqmcBZOo%2Bjxyy
28yQv4vkkTeL5clHEdlKsZ8nKW5vv6dC5aHoNdHf9PjyaaWEokmkqK1a%2BWJOqEs%2BRBKJhhDzkXBU5pZysB%2FRgxKhb4F
5bkagbIpnqFIE9KfUrTc6qXKZF1Rk6g%2B17NOrCtkBBHnyGSYnLrppJSM3jWUja7dh4B2ghCvenkPqk0VsI%2FwAu4%2F8J8
dfAHSy%2B3EK7Zb2%2FivluymPeb%2Bw%2Bpt9e%2FozHPwE%3D&RelayState=cookie%3A1580395259_626f
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 1028
Keep-Alive: timeout=5, max=99
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580395259_626f=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam;
path=/; HttpOnly
Date: Thu, 30 Jan 2020 14:40:59 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-
secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTLjpswFIbX06dA3odbBqaxkkkgpQSpSLhSYqOomcvBJYwlsapuZzNvX5KJGmWlUzaJqvUHgc%2FnOf34xVKS
uGjxp9Y5n8KMFpa19XXGFDxcj1EqOBVfMYU5qUFIxOJ%2FMZ9i3XdxIoUUpKmRNlAKpmeCR4KqtQeYgnlgJj9lshHZAwo7j1
a6p6BsJdimnoaaNaxqWTXTDsVe%2FKcfMc2G1GB3t1KCafr5DvpMi%2BQNTVojJouyZ%2BWZKRmtFGNY0C3rIJTvQwok1BqJ
8%2BXyEqmI7Qow4DQ%2Fkca%2Bpsw9PsPQq1Bf7sNHwaBR6nbN2FKtZBwpQnXI%2BS7vttzv7fLbx7fO%2FiYPANWelJj0%2
BMU8a%2F3xZvcwXs%2BHNRpL3jjCuQ6jCfCUDjD%2Bbc%2FTrDbiP4wCEvdnS7CzkvBo3zOfs1UbxOs%2BUqmcBZOo%2Bjxyy
28yQv4vkkTeL5clHEdlKsZ8nKW5vv6dC5aHoNdHf9PjyaaWEokmkqK1a%2BWJOqEs%2BRBKJhhDzkXBU5pZysB%2FRgxKhb4F
5bkagbIpnqFIE9KfUrTc6qXKZF1Rk6g%2B17NOrCtkBBHnyGSYnLrppJSM3jWUja7dh4B2ghCvenkPqk0VsI%2FwAu4%2F8J8
dfAHSy%2B3EK7Zb2%2FivluymPeb%2Bw%2Bpt9e%2FozHPwE%3D&RelayState=cookie%3A1580395259_626f">here
</a>.</p>
</body></html>

```

Problema 2 di 5

Sommario

Manca un attributo sicuro nella sessione cookie crittografata (SSL)

Severità:	Media
Punteggio CVSS:	6,4
URL:	https://tst-secure.sistemapiemonte.it/conam
Entità:	_shibstate_1580142050_d48c (Cookie)
Rischio:	È possibile intercettare le informazioni relative all'utente e alla sessione (i cookie), inviate durante una sessione crittografata
Cause:	L'applicazione Web invia cookie non sicuri su SSL
Fix:	Aggiungere l'attributo 'Secure' a tutti i cookie sensibili

Differenza:

Motivazione: AppScan ha rilevato che una sessione crittografata (SSL) sta utilizzando un cookie senza l'attributo "secure".

Richieste e risposte del test:

```
GET /conam HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: tst-secure.sistemapiemonte.it
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTLjtMwFibXw1NE3jcXw%2FRitZVKGolIvYQkUyE2leucUkuJHwXnprw9TtqKqkCFZoHAmYjxuXznP78y1rQ
qazJrzEGk8LUBbZxjVQpNuosJapQgkmquiaAVaGIYyWbLbcGuT2oljWSyRM5Ma1CGSxFKoZsKVAbqmTN4ShcTddCmlsTzjDY9
DaxR4Np6Bipac6ikMOBy45X8OfCyA9%2FtZAnm4GotvbvYT9pJ1liNnbtG4oG2TPy3JacWLWteeBd3zEs71Uii4Ama8LFsjJ55
P0HbIRhSz%2FuDtALDff9y96%2BOCDv3%2B0A9YgEfUhmndQCy0ocJMEPax3%2FODHh7kQZ9gTPzgM3KSsx7vuSi4%2BHJfvN
0pSJMPeZ70TjNuQOluPhuApm%2Fsefhxxu1GSMehrnZ0vuw9LAZNSyjdXGG0TdL1Jp5H6TaLwqc0crM4y6P1LImj5XqVR26cb
xfxJtja78nYu2p6C%2FRw%2Bz4%2BmW11KeJ5IkvOvjmszpQvoQJqYIIC5N0UOaecrQdFZ8SwXeDROKGSaqq4bhWBI2XmJ00u
qlynhaUdOoX9azRqw%2FZQgOp8RigjrK1mExL7eJGqaHdsvQNFrgjQtVTmrNGvEP4BXC7%2BE%2BJPj%2F5o9fEe2j3r%2FVX
MV1Oe8n5j9%2Bn19vpnPP00&RelayState=cookie%3A1580142121_926e
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 1000
Keep-Alive: timeout=5, max=100
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580142121_926e=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam;
path=/; HttpOnly
Date: Mon, 27 Jan 2020 16:22:01 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTLjtMwFibXw1NE3jcXw%2FRitZVKGolIvYQkUyE2leucUkuJHwXnprw9TtqKqkCFZoHAmYjxuXznP78y1rQ
qazJrzEGk8LUBbZxjVQpNuosJapQgkmquiaAVaGIYyWbLbcGuT2oljWSyRM5Ma1CGSxFKoZsKVAbqmTN4ShcTddCmlsTzjDY9
DaxR4Np6Bipac6ikMOBy45X8OfCyA9%2FtZAnm4GotvbvYT9pJ1liNnbtG4oG2TPy3JacWLWteeBd3zEs71Uii4Ama8LFsjJ55
P0HbIRhSz%2FuDtALDff9y96%2BOCDv3%2B0A9YgEfUhmndQCy0ocJMEPax3%2FODHh7kQZ9gTPzgM3KSsx7vuSi4%2BHJfvN
0pSJMPeZ70TjNuQOluPhuApm%2Fsefhxxu1GSMehrnZ0vuw9LAZNSyjdXGG0TdL1Jp5H6TaLwqc0crM4y6P1LImj5XqVR26cb
xfxJtja78nYu2p6C%2FRw%2Bz4%2BmW11KeJ5IkvOvjmszpQvoQJqYIIC5N0UOaecrQdFZ8SwXeDROKGSaqq4bhWBI2XmJ00u
qlynhaUdOoX9azRqw%2FZQgOp8RigjrK1mExL7eJGqaHdsvQNFrgjQtVTmrNGvEP4BXC7%2BE%2BJPj%2F5o9fEe2j3r%2FVX
MV1Oe8n5j9%2Bn19vpnPP00&RelayState=cookie%3A1580142121_926e">here</a>.</p>
</body></html>
```

Problema 3 di 5

[Sommario](#)

Manca un attributo sicuro nella sessione cookie crittografata (SSL)

Severità:	Media
Punteggio CVSS:	6,4
URL:	https://tst-secure.sistemapiemonte.it/conam
Entità:	_shibstate_1580395017_f8f7 (Cookie)
Rischio:	È possibile intercettare le informazioni relative all'utente e alla sessione (i cookie), inviate durante una sessione crittografata
Cause:	L'applicazione Web invia cookie non sicuri su SSL
Fix:	Aggiungere l'attributo 'Secure' a tutti i cookie sensibili

Differenza:

Motivazione: AppScan ha rilevato che una sessione crittografata (SSL) sta utilizzando un cookie senza l'attributo "secure".

Richieste e risposte del test:

```
GET /conam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: __utmt=1; __utmb=260743567.1.10.1580394457;
__utma=260743567.231398534.1579858881.1580227032.1580394457.4;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: en-US,en;q=0.5
X-XSRF-TOKEN: 6416026210001487038-407006526009751724

HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTbtiswEIavt09hdB%2BfcqARSSB1DDXk4NreUHoTFHvSCGzJ1ci72bevnAMN6W4oe1Fa3Rhbc%2Fjmnx%2B
PkFV1TaeN3osEfjSA2jpuUB6vBiTRgkqGXKkg1WAVoc0nS7m1LddWiupZS5LYk0RQWkuRSaFNhWofNQQtz%2BExmY%2FJXusa
qeNo1B2EvFFgm3oaK1ZzqKTQYHpt1PzJc9I93251CXpvi0qn7eQ78SrNiDUzaFywtsmfluSs4kWNtWNAd7yEc70ECq4g106ar
ogVzcZk4xf9IWN%2Bse3uun6fDXLoud2eOxz0Bn2v2H40YYgNRAI1E3pMfNd3O67X6XqZ59LekPr9b8SKz3p84qLg4vt98ban
IKSfsyzunGZcg8LjfCaATD6Y8%2FDrjNqN0COHutrR%2FS7sshgyScNkHQXhJk5W62gWJps0DB6T0E6jNAsX0zgKF6t1FtpRt
plHa29jvscj56rpLdDD7fvoZKaloYhmsSx5%2FmJNylI%2BBWqYhjHxiHNT5Jxyth4URYMG7QIP2gpkVTPFsVUEDizXv2lyUe
U6LSjN0Ans3qNRG7aDatTRZ5TlNG%2BrmYTYPJ61KtodG%2B9AkSkmsJZKnzV6DeEfwoXiPyH%2B2neHyy%2F3005Z769ivpv
ylPeG3SeX2%2Buf8eQn&RelayState=cookie%3A1580467765_bc6c
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 996
Keep-Alive: timeout=5, max=99
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580467765_bc6c=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam;
path=/; HttpOnly
Date: Fri, 31 Jan 2020 10:49:25 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-
secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTbtiswEIavt09hdB%2BfcqARSSB1DDXk4NreUHoTFHvSCGzJ1ci72bevnAMN6W4oe1Fa3Rhbc%2Fjmnx%2B
PkFV1TaeN3osEfjSA2jpuUB6vBiTRgkqGXKkg1WAVoc0nS7m1LddWiupZS5LYk0RQWkuRSaFNhWofNQQtz%2BExmY%2FJXusa
qeNo1B2EvFFgm3oaK1ZzqKTQYHpt1PzJc9I93251CXpvi0qn7eQ78SrNiDUzaFywtsmfluSs4kWNtWNAd7yEc70ECq4g106ar
ogVzcZk4xf9IWN%2Bse3uun6fDXLoud2eOxz0Bn2v2H40YYgNRAI1E3pMfNd3O67X6XqZ59LekPr9b8SKz3p84qLg4vt98ban
IKSfsyzunGZcg8LjfCaATD6Y8%2FDrjNqN0COHutrR%2FS7sshgyScNkHQXhJk5W62gWJps0DB6T0E6jNAsX0zgKF6t1FtpRt
plHa29jvscj56rpLdDD7fvoZKaloYhmsSx5%2FmJNylI%2BBWqYhjHxiHNT5Jxyth4URYMG7QIP2gpkVTPFsVUEDizXv2lyUe
U6LSjN0Ans3qNRG7aDatTRZ5TlNG%2BrmYTYPJ61KtodG%2B9AkSkmsJZKnzV6DeEfwoXiPyH%2B2neHyy%2F3005Z769ivpv
ylPeG3SeX2%2Buf8eQn&RelayState=cookie%3A1580467765_bc6c">here</a>.</p>
</body></html>
```

Manca un attributo sicuro nella sessione cookie crittografata (SSL)

Severità:	Media
Punteggio CVSS:	6,4
URL:	https://tst-secure.sistemapiemonte.it/conam
Entità:	_shibstate_1580223803_67de (Cookie)
Rischio:	È possibile intercettare le informazioni relative all'utente e alla sessione (i cookie), inviate durante una sessione crittografata
Cause:	L'applicazione Web invia cookie non sicuri su SSL
Fix:	Aggiungere l'attributo 'Secure' a tutti i cookie sensibili

Differenza:

Motivazione: AppScan ha rilevato che una sessione crittografata (SSL) sta utilizzando un cookie senza l'attributo "secure".

Richieste e risposte del test:

```
GET /conam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: __utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utms=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: en-US,en;q=0.5
X-XSRF-TOKEN: 6416026210001487038-407006526009751724

HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTbjtowEIavt08R%2BZ6ctqVgARINKRoJlJtJoqo3yDiTYimxU4%2FZZd%2B%2BDgcV0RZVe1GlvokSz%2BG
bf35lhKypWzrdma3M4Ns00Dj7ppZIDxdjstOSKoYCqWQNIIDwc5tPFnIauTlutjOKqJs4UEbQRSkZK4q4BnYN%2BEhws%2FmY
b1lpkXqeQdND4DsNrq1noGGtgEZJA64wXi2eAi%2Ffis1G1WC2LqLyuk6hly7zgJgziYk65r8aUnBGLG22HoWtBI1nOplUAo
N3Hh5viROMhuT9cB%2FP6wGg37FgkE57PfdQvL9Pme8Kv17XoU2DHEHiUTDpBmt0A%2F9nh%2F07oMi8OnbIQ37X4iTnvT4IG
Qp5Nfb4m2OQUG%2FFkXa0864Ao2H%2BWWAmbyx5%2B7HGxUboQcOfbGj213YeTFkksfZKonidZotV8ksztZ5HDlmsZsneREvp
mkSL5YPReWmxXqerIK1%2FZ6OvIum10B31%2B%2Bjo5keLEUyS1Ut%2BIszrWv1HGlgBsYkIN5VkvPKyXpQHowYdQvcGydSTc
u0wE4R2DNuftLkrMplWlTboTOoXqNRF1ZBCfrgM8o45V0lm5Dax7PSZbdj6x0oc80ktkqbk0a%2FQvgHcIX8T4g%2Fv%2FOHD
59uod2y3l%2FFFDXlMe83dp%2Bcby9%2FxpPv&RelayState=cookie%3A1580467766_9c48
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 1014
Keep-Alive: timeout=5, max=100
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580467766_9c48=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam;
path=/; HttpOnly
Date: Fri, 31 Jan 2020 10:49:26 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTbjtowEIavt08R%2BZ6ctqVgARINKRoJlJtJoqo3yDiTYimxU4%2FZZd%2B%2BDgcV0RZVe1GlvokSz%2BG
bf35lhKypWzrdma3M4Ns00Dj7ppZIDxdjstOSKoYCqWQNIIDwc5tPFnIauTlutjOKqJs4UEbQRSkZK4q4BnYN%2BEhws%2FmY
b1lpkXqeQdND4DsNrq1noGGtgEZJA64wXi2eAi%2Ffis1G1WC2LqLyuk6hly7zgJgziYk65r8aUnBGLG22HoWtBI1nOplUAo
N3Hh5viROMhuT9cB%2FP6wGg37FgkE57PfdQvL9Pme8Kv17XoU2DHEHiUTDpBmt0A%2F9nh%2F07oMi8OnbIQ37X4iTnvT4IG
Qp5Nfb4m2OQUG%2FFkXa0864Ao2H%2BWWAmbyx5%2B7HGxUboQcOfbGj213YeTFkksfZKonidZotV8ksztZ5HDlmsZsneREvp
mkSL5YPReWmxXqerIK1%2FZ6OvIum10B31%2B%2Bjo5keLEUyS1Ut%2BIszrWv1HGlgBsYkIN5VkvPKyXpQHowYdQvcGydSTc
u0wE4R2DNuftLkrMplWlTboTOoXqNRF1ZBCfrgM8o45V0lm5Dax7PSZbdj6x0oc80ktkqbk0a%2FQvgHcIX8T4g%2Fv%2FOHD
59uod2y3l%2FFFDXlMe83dp%2Bcby9%2FxpPv&RelayState=cookie%3A1580467766_9c48">here</a>.</p>
```

</body></html>

Problema 5 di 5

[Sommaro](#)

Manca un attributo sicuro nella sessione cookie crittografata (SSL)

Severità:	Media
Punteggio CVSS:	6,4
URL:	https://tst-secure.sistemapiemonte.it/conam/
Entità:	XSRF-TOKEN (Cookie)
Rischio:	È possibile intercettare le informazioni relative all'utente e alla sessione (i cookie), inviate durante una sessione crittografata
Cause:	L'applicazione Web invia cookie non sicuri su SSL
Fix:	Aggiungere l'attributo 'Secure' a tutti i cookie sensibili

Differenza:

Motivazione: AppScan ha rilevato che una sessione crittografata (SSL) sta utilizzando un cookie senza l'attributo "secure".

Richieste e risposte del test:

```
GET /conam/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam
Cookie: __utma=32890173.1526803074.1567412775.1567412775.1567412775.1;
_shibsession_rpplivlIRUP= 802eddf8c7ca08c71757be2deb189387;
__utmz=32890173.1567412775.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTbtswEIavt09hdB%2BfKpJGJIHUMdSQg2t7Q%2B1NUORJI7AlVyPvbt%2B%2Bcg40pG0oelFa3Rhbc%2Fj
mnx%2BPKdVQ2etOcgMvraAxpmpK4n0eDEhrZZUMRRIJasBqeE0ny0XNHR92mhlFFCvCwaIoI1QM1IS2xp0DvpJcHjMFhNyMK
ZB6nkGTQ%2BBtxpcW89AzRoBtZIGXGG8SjwFXn4Qu52qwBxcROV1nUIvXecFceYWTUjWNfnTkoLVomyw8SzoX1RwrpdBKTRw4
%2BX5mjJfEK2vj9knPV3%2FRCgH44Go%2BGAj8r9O7bjUJaJ0oYhtpBINEyaCQn900%2F5Qa%2FvF8GADgLqDz8TJz3r8V7I
Usgv98XbnYKQfiiKtHeacQMaj%2FPZADJ9Y8%2FDjzPuNkKPHPPqR%2Fe7sMtiyDSPs00Sxds0W2%2BSeZxt8zh6zGI3T%2FI
iXs7SJF6uV0XsJsV2kWyCrF2ejr2rprdAD7fv45OZVpYimaegEvybM6sq9RxpYAYmJCDeTZFzyt16UB6NGHULfDFOpOqGaYGd
IvDCuPlJk4sq121RZYfOYP8ajbqWPZSgJz6jjFPeVbMJqX08K11207begbLQTKGktDlr9CuEfWbXyP%2BE%2BNNbf7T6eA%2F
tnvX%2BKuarKU95v7H79HJ7%2FT0efgc%3D&RelayState=cookie%3A1580395267_8d9f
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 1012
Keep-Alive: timeout=5, max=83
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580395267_8d9f=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam%2F;
path=/; HttpOnly
Date: Thu, 30 Jan 2020 14:41:07 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
```

```
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?SAMLRequest=1ZTbitswEIavt09hdB%2BfKpJGJIHUMdSQg2t7Q%2B1NUORJI7A1VyPvbt%2B%2Bcg40pG0oe1Fa3Rhbc%2Fjmnx%2BPkdVVQ2etOcgMvraAxxnpK4n0eDEhrZZUMRRIJasBqeE0ny0XNHR92mhlFFcVcWaIoI1QM1IS2xp0DvpJcHjMFhNyMKZB6nkGTQ%2BBtxpcW89AzRoBtZIGXGG8SjwFXn4Qu52qwBxcROV1nUIvXecFceYWTUjWNfnTkoLVomyw8SzoX1RwrpdBKTRw4%2BX5mjJjFfEK2vj9knPV3%2FRCgH44Go%2BGAj8r9O7bjUJaJ0oYhtpBINEyaCQn900%2F5Qa%2FvF8GADgLqDz8TJz3r8V7IUs9v98XbnYKQfiiKtHeacQMaj%2FPZADJ9Y8%2FDjzPuNkKPHPPqR%2Fe7sMtiyDSPs00Sxds0W2%2BSeZxt8zh6zGI3T%2FIiXs7SJF6uV0XsJsV2kWyCrf2ejr2rprdAD7fv45OZVpYimaeqEvybM6sq9RxpYAYmJCDeTZFzyt16UB6NGHULfDFOpOqGaYGdIvDCuPlJk4sq12lRZYfOYP8ajbqwPZSgJz6jjjFPeVbMJqX08K11207begbLQTKGjtDlr9CuEfWBXyP%2BE%2BNNbf7T6eA%2FtnvX%2BKuarKU95v7H79HJ7%2FTOfgc%3D&RelayState=cookie%3A1580395267_8d9f">here</a>.</p>
</body></html>
```

Problema 1 di 4

Sommar

Intestazione "Content-Security-Policy" mancante o non sicura

Severità: **Bassa**

Punteggio CVSS: 5,0

URL: <https://tst-secure.sistemapiemonte.it/conam>

Entità: conam (Page)

Rischio: È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
 È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause: Programmazione o configurazione non sicura dell'applicazione Web**Fix:** Configurare il server per l'utilizzo dell'intestazione "Content-Security-Policy" con politiche sicure**Differenza:**

Motivazione: AppScan ha rilevato che l'intestazione della risposta Content-Security-Policy non è presente o ha una politica non sicura, e questo aumenta l'esposizione a vari attacchi iniezione di tipo cross-site

Richieste e risposte del test:

```
GET /conam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: tst-secure.sistemapiemonte.it
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTbjtowEIavt08R%2BZ6cuiXgARINKRoJlJtJoqo3yCSTYimxU4%2Bzy759HQ4qoi2q9qJqfRmlnsM3%2F%2FzKGFldNXTW6p1I4FsLqK19XQmkh4sJaZWgkiFHKlgNSHVO09lyQX3bpY2SWuayitYMEZTmUgRSYFuDSkE98xyeksWE7LRukDqORtlDyFsFtqmnoWYNhloKDTbXTsWfPSfd8e1WVqB3NqJ0uk6%2BE6%2FSjFhzg8YF65r8aUnOal402DgGtOQVnOolUHAfUXbSdEwsaD4hg3hg22HxfGajKEf3Zd%2BF%2Fn3J%2BsPRlvXcwXBkwhBbiARqJvSE%2BK7v9lyv5w8y74H6PnW9L8SKT3p84KLg4utt8bbHIKQfsyzuHWdcg8LDfCaATN%2BZc%2FfjjLuN0AOHutjR7S7svBgyTcNkHQXhJk5W62geJps0DJ6S0E6jNAuXszgKl6vHLLSjbLOIlt7GfI%2FHzkXTa6C76%2Ffx0UyPhiKax7Li%2Baslqyr5EihgGibEI85VkvPKyXpQHIwYdAvcaYuQdcMUX04R2Lnc%2F6TJWZXLtKAYQydQvKwJLqyEATBZ5TlN0%2BqmYTYPF6kKrodG%2B9AkSkmsJfKnzT6FcI%2FgMvFf0L8ue%2BOHj%2FQrtlvb%2BK%2BWBKY95v7D49317%2BjKfAQ%3D%3D&RelayState=cookie%3A1580142121_ecaa
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 1022
Keep-Alive: timeout=5, max=99
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580142121_ecaa=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam;
```

```

path=/; HttpOnly
Date: Mon, 27 Jan 2020 16:22:01 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?SAMLRequest=1ZTbtjtoWEIavt08R%2BZ6cuiXgARiNkRoJlJtJoqo3yCSTYimxU4%2Bzy759HQ4qoi2q9qJqfRmLnsM3%2F%2FzKGfLdNXTW6p1I4FsLqK19XQmkh4sJaZWgkiFHKlgNSHVO09lyQX3bpY2SWuayItYMEZTmUgRSYFuDSkE98xyeksWE7LRukDqOrt1DyFsFtgmnoWYNhloKDTbXTsWfPSfd8e1WVqB3NqJ0uk6%2BE6%2FSjFhzg8YF65r8aUnOal402DgGtOQVnOolUHAfuXbSgEWsaD4hg3hg22HxfGajKEf3Zd%2BF%2Fn3J%2BsPRlvXcwXBkwBbiARqJvSE%2BK7v9lyv5w8y74H6PnW9L8SKT3p84KLg4utt8bbHIKQfsyzuHWdcg8LDfCaATN%2BZc%2FfjJLuN0AOHutjR7S7svBgyTcNkHQXhJk5W62geJps0DJ6S0E6jNAuXszgK16vHLLSjbLOIlt7GfI%2FHzkXTa6C76%2Ffx0UyPhiKax7Li%2Baslqyr5EingGibEI85VkvPKyXpQHlwYdAvcaYuQdcMUX04R2Lnc%2F6TJWZXLtKAYQydQvkWjLqyEAtTBZ5TlNO%2BqmYTYPF6kKrodG%2B9AkSkmsJFKnzT6FcI%2FgMvFf0L8ue%2BOHj%2FdQrtlvb%2BK%2BWbKY95v7D49317%2BjKfAQ%3D%3D&RelayState=cookie%3A1580142121_ecaa">here</a>.
</p>
</body></html>

```

Problema 2 di 4

[Sommaro](#)

Intestazione "Content-Security-Policy" mancante o non sicura

Severità: Bassa

Punteggio CVSS: 5,0

URL: <https://tst-secure.sistemapiemonte.it/conam/inline.bundle.js>

Entità: inline.bundle.js (Page)

Rischio: È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause: Programmazione o configurazione non sicura dell'applicazione Web

Fix: Configurare il server per l'utilizzo dell'intestazione "Content-Security-Policy" con politiche sicure

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta Content-Security-Policy non è presente o ha una politica non sicura, e questo aumenta l'esposizione a vari attacchi iniezione di tipo cross-site

Richieste e risposte del test:

```

GET /conam/inline.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliviSISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utms=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

```


X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK

Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT

Connection: Keep-Alive

Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40

Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it

Accept-Ranges: bytes

Pragma: no-cache

Vary: Accept-Encoding,User-Agent

Content-Length: 1370

Keep-Alive: timeout=5, max=88

Cache-Control: no-cache, no-store, must-revalidate

Strict-Transport-Security: max-age=0

ETag: W/"1370-1579614182000"

Date: Thu, 30 Jan 2020 14:41:07 GMT

Expires: 0

Content-Type: text/javascript

```
!function(e){function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}var r=window.webpackJsonp;window.webpackJsonp=function(t,c,u){for(var a,i,f,l=0,s=[];l<t.length;l++)i=t[l],o[i]&&s.push(o[i][0]),o[i]=0;for(a in c)Object.prototype.hasOwnProperty.call(c,a)&&(e[a]=c[a]);for(r&&r(t,c,u);s.length;)s.shift();if(u)for(l=0;l<u.length;l++)f=n(u.s=u[l]);return f;var t={},o={5:0};n.e=function(e){function r(){a.onerror=a.onload=null,clearTimeout(i);var n=o[e];0!==n&&(n&&n[1](new Error("Loading chunk "+e+" failed.")),o[e]=void 0);var t=o[e];if(0===t)return new Promise(function(e){e()});if(t)return t[2];var c=new Promise(function(n,r){t=o[e]=[n,r]});t[2]=c;var u=document.getElementsByTagName("head")[0],a=document.createElement("script");a.type="text/javascript",a.charset="utf-8",a.async=!0,a.timeout=12e4,n.nc&&a.setAttribute("nonce",n.nc),a.src=n.p+""+e+ ".chunk.js";var i=setTimeout(r,12e4);return a.onerror=a.onload=r,u.appendChild(a),c,n.m=e,n.c=t,n.d=function(e,r,t){n.o(e,r)||Object.defineProperty(e,r,{configurable:!1,enumerable:!0,get:t})},n.n=function(e){var r=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(r,"a",r),r),n.o=function(e,n){return Object.prototype.hasOwnProperty.call(e,n)},n.p="/conam/",n.oe=function(e){throw console.error(e),e}}{}};
```

Problema 3 di 4

[Sommario](#)

Intestazione "Content-Security-Policy" mancante o non sicura

Severità: **Bassa**

Punteggio CVSS: 5,0

URL: <https://tst-secure.sistemapiemonte.it/conam/styles.bundle.js>

Entità: styles.bundle.js (Page)

Rischio: È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause: Programmazione o configurazione non sicura dell'applicazione Web

Fix: Configurare il server per l'utilizzo dell'intestazione "Content-Security-Policy" con politiche sicure

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta Content-Security-Policy non è presente o ha una politica non sicura, e questo aumenta l'esposizione a vari attacchi

iniezione di tipo cross-site

Richieste e risposte del test:

```
GET /conam/styles.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
_shibsession_spslivlSISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 179718
Keep-Alive: timeout=5, max=71
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"179718-1579614182000"
Date: Thu, 30 Jan 2020 14:41:08 GMT
Expires: 0
Content-Type: text/javascript

webpackJsonp([2],{"/node_modules/bootstrap/dist/css/bootstrap.min.css":function(e,o,t){var
r=t("./node_modules/css-loader/index.js?
{"sourceMap":false,"importLoaders":1)!./node_modules/postcss-loader/index.js?
{"ident":"postcss"}!./node_modules/bootstrap/dist/css/bootstrap.min.css");"string"==typeof r&&(r=
[[e.i,r,""]]);t("./node_modules/style-loader/addStyles.js")(r,{});r.locals&&
(e.exports=r.locals)},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.eot":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.f4769f9bdb7466be6508.eot"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.svg":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.89889688147bd7575d63.svg"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.ttf":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.e18bbf611f2a2e43afc0.ttf"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.woff":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.f2772327f55d8198301.woff"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.woff2":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.448c34a56d699c29117a.woff2"},'./node_modules/css-loader/index.js?
{"sourceMap":false,"importLoaders":1)!./node_modules/postcss-loader/index.js?
{"ident":"postcss"}!./node_modules/bootstrap/dist/css/bootstrap.min.css':function(e,o,t){var
r=t("./node_modules/css-loader/lib/url/escape.js");o=e.exports=t("./node_modules/css-
loader/lib/css-base.js")(!1),o.push([e.i,'/*!\n * Bootstrap v3.4.1 (https://getbootstrap.com/)\n
* Copyright 2011-2019 Twitter, Inc.\n * Licensed under MIT
(https://github.com/twbs/bootstrap/blob/master/LICENSE)\n */\n\n normalize.css v3.0.3 | MIT
License | github.com/necolas/normalize.css */html{font-family:sans-serif;-ms-text-size-
adjust:100%;-webkit-text-size-
adjust:100%;body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,
nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-
align:baseline}audio:not([controls]){display:none;height:0}
[hidden],template{display:none}a{background-
color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:none;text-
decoration:underline;-webkit-text-decoration:underline dotted;-moz-text-decoration:underline
dotted;text-decoration:underline dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-
size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-
size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-
.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{box-sizing:content-
box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-
size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflo
w:visible}button,select{text-transform:none}button,html
input[type=button],input[type=reset],input[type=submit]{-webkit-
appearance:button;cursor:pointer}button[disabled],html input[disabled]{cursor:default}button::-
moz-focus-inner,input::-moz-focus-inner{border:0;padding:0}input{line-
height:normal}input[type=checkbox],input[type=radio]{box-sizing:border-
```

```

box;padding:0}input[type=number]::-webkit-inner-spin-button,input[type=number]::-webkit-outer-
spin-button{height:auto}input[type=search]{-webkit-appearance:textfield;box-sizing:content-
box}input[type=search]::-webkit-search-cancel-button,input[type=search]::-webkit-search-
decoration{-webkit-appearance:none}fieldset{border:1px solid silver;margin:0 2px;padding:.35em
.625em .
...
...
...

```

Problema 4 di 4

Sommario

Intestazione "Content-Security-Policy" mancante o non sicura

Severità:

Bassa

Punteggio CVSS: 5,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/polyfills.bundle.js>

Entità:

polyfills.bundle.js (Page)

Rischio:

È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause:

Programmazione o configurazione non sicura dell'applicazione Web

Fix:

Configurare il server per l'utilizzo dell'intestazione "Content-Security-Policy" con politiche sicure

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta Content-Security-Policy non è presente o ha una politica non sicura, e questo aumenta l'esposizione a vari attacchi iniezione di tipo cross-site

Richieste e risposte del test:

```

GET /conam/polyfills.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

```

```

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 162079
Keep-Alive: timeout=5, max=70
Cache-Control: no-cache, no-store, must-revalidate

```

```

Strict-Transport-Security: max-age=0
ETag: W/"162079-1579614182000"
Date: Thu, 30 Jan 2020 14:41:09 GMT
Expires: 0
Content-Type: text/javascript

webpackJsonp([1],{["./node_modules/classlist.js/classList.js":function(e,o){/*! @source
http://purl.eligrey.com/github/classList.js/blob/master/classList.js */
"document"in self&&("classList"in document.createElement("_")&&
(!document.createElementNS||"classList"in
document.createElementNS("http://www.w3.org/2000/svg","g"))?function(){var e="use strict";var
e=document.createElement("_");if(e.classList.add("c1","c2"),!e.classList.contains("c2")){var
o=function(e){var o=DOMTokenList.prototype[e];DOMTokenList.prototype[e]=function(e){var
s,t=arguments.length;for(s=0;s<t;s++)e=arguments[s],o.call(this,e)};o("add"),o("remove")}if(e.cl
assList.toggle("c3",!1),e.classList.contains("c3")){var
s=DOMTokenList.prototype.toggle;DOMTokenList.prototype.toggle=function(e,o){return 1 in
arguments&&!this.contains(e)==!o?o:s.call(this,e)}e=null}():function(e){var e="use
strict";if("Element"in e){var o=e.Element.prototype,s=Object,t=String.prototype.trim||function()
{return this.replace(/^\s+|\s+$/g,"")},n=Array.prototype.indexOf||function(e){for(var
o=0,s=this.length;o<s;o++)if(o in this&&this[o]===e)return o;return-1},r=function(e,o)
{this.name=e,this.code=DOMException[e],this.message=o,u=function(e,o){if("==="o)throw new
r("SYNTAX_ERR","An invalid or illegal string was specified");if(/\/s/.test(o))throw new
r("INVALID_CHARACTER_ERR","String contains an invalid character");return
n.call(e,o)},d=function(e){for(var o=t.call(e.getAttribute("class"))||""),s=o?o.split(/\s+/):
[],n=0,r=s.length;n<r;n++)this.push(s[n]);this._updateClassName=function()
{e.setAttribute("class",this.toString())},l=d.prototype=[],c=function(){return new
d(this)};if(r.prototype=Error.prototype,l.item=function(e){return
this[e]||null},l.contains=function(e){return e+="",!1===u(this,e)},l.add=function(){var
e,o=arguments,s=0,t=o.length,n=!1;do{e=o[s]+ "",-1===u(this,e)&&
(this.push(e),n=!0)}while(++s<t);n&&this._updateClassName();l.remove=function(){var
e,o,s=arguments,t=0,n=s.length,r=!1;do{for(e=s[t]+ "",o=u(this,e);-
1!==o;)this.splice(o,1),r=!0,o=u(this,e)}while(++t<n);r&&this._updateClassName();l.toggle=functi
on(e,o){e+ "";var s=this.contains(e),t=s?!0!==o&&"remove":!1!==o&&"add";return t&&this[t]
(e),!0===o||!1===o?o:!s},l.toString=function(){return this.join(" ")},s.defineProperty({var i=
{get:c,enumerable:!0,configurable:!0};try{s.defineProperty(o,"classList",i)}catch(e){-
2146823252===e.number&&(i.enumerable=!1,s.defineProperty(o,"classList",i))}}else
s.prototype.__defineGetter__&&o.__defineGetter__("classList",c)}(self)}),["./node_modules/core-
js/es6/array.js":function(e,o,s){s(["./node_modules/core-
js/modules/es6.string.iterator.js"),s(["./node_modules/core-js/modules/es6.array.is-
array.js"),s(["./node_modules/core-js/modules/es6.array.from.js"),s(["./node_modules/core-
js/modules/es6.array.of.js"),s(["./node_modules/core-
js/modules/es6.array.join.js"),s(["./node_modules/core-
js/modules/es6.array.slice.js"),s(["./node_modules/core-
js/modules/es6.array.sort.js"),s(["./node_modules/core-js/modules/es6.array.for-
each.js"),s(["./node_modules/core-js/modules/es6.array.map.js"),s(["./node_modules/core-
js/modules/es6.array.filter.js"),s(["./node_modules/core-
js/modules/es6.array.some.js"),s(["./node_modules/core-
js/modules/es6.array.every.js"),s(["./node_modules/core-
js/modules/es6.array.reduce.js"),s(["./node_modules/core-js/modules/es6.array.reduce-
right.js"),s(["./node_modules/core-js/modules/es6.array.index-of.js"),s(["./node_modules/core-
js/modules/es6.array.last-index-of.js"),s(["./node_modules/core-js/modules/es6.array.copy-
within.js"),s(["./node_modules/core-js/modules/es6.array.fill.js"),s(["./node_modules/core-
...
...
...

```

Intestazione "X-Content-Type-Options" mancante o non sicura

Severità:

Bassa

Punteggio CVSS: 5,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/inline.bundle.js>

Entità:

inline.bundle.js (Page)

Rischio:

È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause:

Programmazione o configurazione non sicura dell'applicazione Web

Fix:

Configurare il server per l'utilizzo dell'intestazione "X-Content-Type-Options" con il valore "nosniff"

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta "X-Content-Type-Options" non è presente o ha un valore non sicuro, e questo aumenta l'esposizione ad attacchi download di tipo drive-by

Richieste e risposte del test:

```
GET /conam/inline.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
_shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcid=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 1370
Keep-Alive: timeout=5, max=88
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"1370-1579614182000"
Date: Thu, 30 Jan 2020 14:41:07 GMT
Expires: 0
Content-Type: text/javascript

!function(e){function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}var r=window.webpackJsonp;window.webpackJsonp=function(t,c,u){for(var a,i,f,l=0,s=[];l<t.length;l++)i=t[l],o[i]&&s.push(o[i][0]),o[i]=0;for(a in c)Object.prototype.hasOwnProperty.call(c,a)&&(e[a]=c[a]);for(r&&r(t,c,u);s.length;)s.shift();if(u)for(l=0;l<u.length;l++)f=n(u[l]);return f;var t={},o={5:0};n.e=function(e){function r(){a.onerror=a.onload=null,clearTimeout(i);var n=o[e];0!==n&&(n&&n[1](new Error("Loading chunk "+e+" failed.")),o[e]=void 0)}var t=o[e];if(0===t)return new Promise(function(e){e()});if(t)return t[2];var c=new Promise(function(n,r){t=o[e]=[n,r]});t[2]=c;var u=document.getElementsByTagName("script")[0],a=document.createElement("script");a.type="text/javascript",a.charset="utf-8",a.async=!0,a.timeout=12e4,n.nc&&a.setAttribute("nonce",n.nc),a.src=n.p+""+e+".chunk.js";var
```

```
i=setTimeout(r,12e4);return
a.onerror=a.onload=r,u.appendChild(a),c},n.m=e,n.c=t,n.d=function(e,r,t)
{n.o(e,r)||Object.defineProperty(e,r,{configurable:!1,enumerable:!0,get:t})},n.n=function(e){var
r=e&&e.__esModule?function(){return e.default}:function(){return e};return
n.d(r,"a",r),r),n.o=function(e,n){return
Object.prototype.hasOwnProperty.call(e,n)},n.p="/conam/",n.oe=function(e){throw
console.error(e),e}}([]);
```

Problema 2 di 4

[Sommarlo](#)

Intestazione "X-Content-Type-Options" mancante o non sicura

Severità:	Bassa
Punteggio CVSS:	5,0
URL:	https://tst-secure.sistemapiemonte.it/conam/styles.bundle.js
Entità:	styles.bundle.js (Page)
Rischio:	È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.
Cause:	Programmazione o configurazione non sicura dell'applicazione Web
Fix:	Configurare il server per l'utilizzo dell'intestazione "X-Content-Type-Options" con il valore "nosniff"

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta "X-Content-Type-Options" non è presente o ha un valore non sicuro, e questo aumenta l'esposizione ad attacchi download di tipo drive-by

Richieste e risposte del test:

```
GET /conam/styles.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180
```

```
HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 179718
Keep-Alive: timeout=5, max=71
Cache-Control: no-cache, no-store, must-revalidate
```

```

Strict-Transport-Security: max-age=0
ETag: W/"179718-1579614182000"
Date: Thu, 30 Jan 2020 14:41:08 GMT
Expires: 0
Content-Type: text/javascript

webpackJsonp([2],{["./node_modules/bootstrap/dist/css/bootstrap.min.css":function(e,o,t){var
r=t("./node_modules/css-loader/index.js?
{"sourceMap":false,"importLoaders":1}!./node_modules/postcss-loader/index.js?
{"ident":"postcss"}!./node_modules/bootstrap/dist/css/bootstrap.min.css');"string"==typeof r&&(r=
[[e.i,r,""]]);t("./node_modules/style-loader/addStyles.js")(r,{});r.locals&&
(e.exports=r.locals)},["./node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.eot":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.f4769f9bdb7466be6508.eot"},["./node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.svg":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.89889688147bd7575d63.svg"},["./node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.ttf":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.el8bbf611f2a2e43afc0.ttf"},["./node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.woff":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.fa2772327f55d8198301.woff"},["./node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.woff2":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.448c34a56d699c29117a.woff2"}],["./node_modules/css-loader/index.js?
{"sourceMap":false,"importLoaders":1}!./node_modules/postcss-loader/index.js?
{"ident":"postcss"}!./node_modules/bootstrap/dist/css/bootstrap.min.css":function(e,o,t){var
r=t("./node_modules/css-loader/lib/url/escape.js");o=e.exports=t("./node_modules/css-
loader/lib/css-base.js")(!1),o.push([e.i,'/*!\n * Bootstrap v3.4.1 (https://getbootstrap.com/)\n
* Copyright 2011-2019 Twitter, Inc.\n * Licensed under MIT
(https://github.com/twbs/bootstrap/blob/master/LICENSE)\n *//*! normalize.css v3.0.3 | MIT
License | github.com/necolas/normalize.css */html{font-family:sans-serif;-ms-text-size-
adjust:100%;-webkit-text-size-
adjust:100%;body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,
nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-
align:baseline}audio:not([controls]){display:none;height:0}
[hidden],template{display:none}a{background-
color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:none;text-
decoration:underline;-webkit-text-decoration:underline dotted;-moz-text-decoration:underline
dotted;text-decoration:underline dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-
size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-
size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-
.25em}img{border:0;svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{box-sizing:content-
box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-
size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflo
w:visible}button,select{text-transform:none}button,html
input[type=button],input[type=reset],input[type=submit]{-webkit-
appearance:button;cursor:pointer}button[disabled],html input[disabled]{cursor:default}button::-
moz-focus-inner,input::-moz-focus-inner{border:0;padding:0}input{line-
height:normal}input[type=checkbox],input[type=radio]{box-sizing:border-
box;padding:0}input[type=number]::-webkit-inner-spin-button,input[type=number]::-webkit-outer-
spin-button{height:auto}input[type=search]{-webkit-appearance:textfield;box-sizing:content-
box}input[type=search]::-webkit-search-cancel-button,input[type=search]::-webkit-search-
decoration{-webkit-appearance:none}fieldset{border:1px solid silver;margin:0 2px;padding:.35em
.625em .
...
...
...

```

Intestazione "X-Content-Type-Options" mancante o non sicura

Severità: **Bassa**

Punteggio CVSS: 5,0

URL: <https://tst-secure.sistemapiemonte.it/conam/polyfills.bundle.js>

Entità: polyfills.bundle.js (Page)

Rischio: È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause: Programmazione o configurazione non sicura dell'applicazione Web

Fix: Configurare il server per l'utilizzo dell'intestazione "X-Content-Type-Options" con il valore "nosniff"

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta "X-Content-Type-Options" non è presente o ha un valore non sicuro, e questo aumenta l'esposizione ad attacchi download di tipo drive-by

Richieste e risposte del test:

```
GET /conam/polyfills.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
_shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.1.utmcsr=(direct)|utmccn=(direct)|utmcid=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 162079
Keep-Alive: timeout=5, max=70
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"162079-1579614182000"
Date: Thu, 30 Jan 2020 14:41:09 GMT
Expires: 0
Content-Type: text/javascript

webpackJsonp([1],{"/node_modules/classlist.js/classList.js":function(e,o){/*! @source
http://purl.eligrey.com/github/classList.js/blob/master/classList.js */
"document"in self&&("classList"in document.createElement("_"))&&
(!document.createElementNS||"classList"in
document.createElementNS("http://www.w3.org/2000/svg","g"))?function(){var
e=document.createElement("_");if(e.classList.add("c1","c2"),!e.classList.contains("c2")){var
o=function(e){var o=DOMTokenList.prototype[e];DOMTokenList.prototype[e]=function(e){var
s,t=arguments.length;for(s=0;s<t;s++)e=arguments[s],o.call(this,e)};o("add"),o("remove")}if(e.cl
assList.toggle("c3",!1),e.classList.contains("c3")){var
s=DOMTokenList.prototype.toggle;DOMTokenList.prototype.toggle=function(e,o){return 1 in
arguments&&!this.contains(e)==!o?o:s.call(this,e)}e=null}():function(e){var
strict;if("Element"in e){var o=e.Element.prototype,s=Object,t=String.prototype.trim||function()
strict;if("Element"in e){var o=e.Element.prototype,s=Object,t=String.prototype.trim||function()
```



```

{return this.replace(/^\\s+|\\s+$/g, "")}, n=Array.prototype.indexOf||function(e){for(var
o=0,s=this.length;o<s;o++)if(o in this&&this[o]===e)return o;return-1}, r=function(e,o)
{this.name=e, this.code=DOMException[e], this.message=o}, u=function(e,o){if(" "==o)throw new
r("SYNTAX_ERR", "An invalid or illegal string was specified"); if(/\\s/.test(o))throw new
r("INVALID_CHARACTER_ERR", "String contains an invalid character"); return
n.call(e,o)}, d=function(e){for(var o=t.call(e.getAttribute("class"))||"", s=o.split(/\\s+/):
[], n=0, r=s.length; n<r; n++)this.push(s[n]); this._updateClassName=function()
{e.setAttribute("class", this.toString())}, l=d.prototype=[], c=function() {return new
d(this)}; if(r.prototype=Error.prototype, l.item=function(e){return
this[e]||null}, l.contains=function(e){return e+="", -1!==u(this, e)}, l.add=function() {var
e,o=arguments, s=0, t=o.length, n=!1; do{e=o[s]+ "", -1!==u(this, e) &&
(this.push(e, n=!0))} while(++s<t); n&&this._updateClassName()}, l.remove=function() {var
e,o,s=arguments, t=0, n=s.length, r=!1; do{for(e=s[t]+ "", o=u(this, e); -
1!==o;) this.splice(o, 1), r=!0, o=u(this, e)} while(++t<n); r&&this._updateClassName(), l.toggle=functi
on(e,o){e+ ""; var s=this.contains(e), t=s?!0!==(o&&"remove":!1!==(o&&"add"); return t&&this[t]
(e), !0===o||!1===o?o:!s}, l.toString=function(){return this.join(" ")}, s.defineProperty({var i=
{get:c, enumerable:!0, configurable:!0}; try{s.defineProperty(o, "classList", i)} catch(e){-
2146823252===e.number&&(i.enumerable=!1, s.defineProperty(o, "classList", i))}} else
s.prototype.__defineGetter__&&o.__defineGetter__("classList", c)}(self)), "/node_modules/core-
js/es6/array.js":function(e,o,s){s("./node_modules/core-
js/modules/es6.string.iterator.js"), s("./node_modules/core-js/modules/es6.array.is-
array.js"), s("./node_modules/core-js/modules/es6.array.from.js"), s("./node_modules/core-
js/modules/es6.array.of.js"), s("./node_modules/core-
js/modules/es6.array.join.js"), s("./node_modules/core-
js/modules/es6.array.slice.js"), s("./node_modules/core-
js/modules/es6.array.sort.js"), s("./node_modules/core-js/modules/es6.array.for-
each.js"), s("./node_modules/core-js/modules/es6.array.map.js"), s("./node_modules/core-
js/modules/es6.array.filter.js"), s("./node_modules/core-
js/modules/es6.array.some.js"), s("./node_modules/core-
js/modules/es6.array.every.js"), s("./node_modules/core-
js/modules/es6.array.reduce.js"), s("./node_modules/core-js/modules/es6.array.reduce-
right.js"), s("./node_modules/core-js/modules/es6.array.index-of.js"), s("./node_modules/core-
js/modules/es6.array.last-index-of.js"), s("./node_modules/core-js/modules/es6.array.copy-
within.js"), s("./node_modules/core-js/modules/es6.array.fill.js"), s("./node_modules/core-
...
...
...

```

Problema 4 di 4

Sommario

Intestazione "X-Content-Type-Options" mancante o non sicura

Severità:

Bassa

Punteggio CVSS: 5,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/>

Entità:

(Page)

Rischio:

È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause:

Programmazione o configurazione non sicura dell'applicazione Web

Fix:

Configurare il server per l'utilizzo dell'intestazione "X-Content-Type-Options" con il valore "nosniff"

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta "X-Content-Type-Options" non è presente o ha un valore non sicuro, e questo aumenta l'esposizione ad attacchi download di tipo drive-by

Richieste e risposte del test:

```
GET /conam/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 832
Keep-Alive: timeout=5, max=53
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"832-1579614182000"
Date: Thu, 30 Jan 2020 14:41:11 GMT
content-security-policy: script-src 'self' 'unsafe-eval';
content-security-policy: script-src 'self' 'unsafe-eval';
Expires: 0
Content-Type: text/html

<!doctype html>
<html lang="it">

<head>
  <meta charset="utf-8">
  <title>conamwcl</title>
  <base href="/conam/">

  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="Content-Security-Policy" content="script-src 'self' 'unsafe-eval'; ">
  <link rel="icon" type="image/x-icon" href="favicon.ico">
</head>

<body>
  <app-root></app-root>
  <script type="text/javascript" src="/conam/inline.bundle.js"></script><script
  type="text/javascript" src="/conam/polyfills.bundle.js"></script><script type="text/javascript"
  src="/conam/scripts.bundle.js"></script><script type="text/javascript"
  src="/conam/styles.bundle.js"></script><script type="text/javascript"
  src="/conam/vendor.bundle.js"></script><script type="text/javascript"
  src="/conam/main.bundle.js"></script></body>

</html>
```

Intestazione "X-XSS-Protection" mancante o non sicura**Severità:** **Bassa****Punteggio CVSS:** 5,0**URL:** <https://tst-secure.sistemapiemonte.it/conam/inline.bundle.js>**Entità:** inline.bundle.js (Page)

Rischio: È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
 È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause: Programmazione o configurazione non sicura dell'applicazione Web**Fix:** Configurare il server per l'utilizzo dell'intestazione "X-XSS-Protection" con il valore '1' (abilitato)**Differenza:**

Motivazione: AppScan ha rilevato che l'intestazione della risposta X-XSS-Protection non è presente o ha un valore non sicuro, e potrebbe consentire attacchi Cross-Site Scripting

Richieste e risposte del test:

```
GET /conam/inline.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 1370
Keep-Alive: timeout=5, max=88
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"1370-1579614182000"
Date: Thu, 30 Jan 2020 14:41:07 GMT
Expires: 0
Content-Type: text/javascript

!function(e){function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}var r=window.webpackJsonp;window.webpackJsonp=function(t,c,u){for(var a,i,f,l=0,s=[];l<t.length;l++)i=t[l],o[i]&&s.push(o[i][0]),o[i]=0;for(a in c)Object.prototype.hasOwnProperty.call(c,a)&&(e[a]=c[a]);for(r&&r(t,c,u);s.length;)s.shift();if(u)for(l=0;l<u.length;l++)f=n(n.s=u[l]);return f};var t={},o={5:0};n.e=function(e){function r(){a.onerror=a.onload=null,clearTimeout(i);var n=o[e];0!==n&&(n&&n[1](new Error("Loading chunk "+e+" failed.")),o[e]=void 0)}var t=o[e];if(0===t)return new Promise(function(e){e()});if(t)return t[2];var c=new Promise(function(n,r){t=o[e]=[n,r]});t[2]=c;var u=document.getElementsByTagName("head")[0],a=document.createElement("script");a.type="text/javascript",a.charset="utf-
```

```
8",a.async=!0,a.timeout=12e4,n.nc&&a.setAttribute("nonce",n.nc),a.src=n.p+""+e+".chunk.js";var
i=setTimeout(r,12e4);return
a.onerror=a.onload=r,u.appendChild(a),c},n.m=e,n.c=t,n.d=function(e,r,t)
{n.o(e,r)||Object.defineProperty(e,r,{configurable:!0,enumerable:!0,get:t})},n.n=function(e){var
r=e&&e.__esModule?function(){return e.default}:function(){return e};return
n.d(r,"a",r),r},n.o=function(e,n){return
Object.prototype.hasOwnProperty.call(e,n)},n.p="/conam/",n.oe=function(e){throw
console.error(e),e}}([]);
```

Problema 2 di 4

Sommario

Intestazione "X-XSS-Protection" mancante o non sicura

Severità:

Bassa

Punteggio CVSS: 5,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/styles.bundle.js>

Entità:

styles.bundle.js (Page)

Rischio:

È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause:

Programmazione o configurazione non sicura dell'applicazione Web

Fix:

Configurare il server per l'utilizzo dell'intestazione "X-XSS-Protection" con il valore '1' (abilitato)

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta X-XSS-Protection non è presente o ha un valore non sicuro, e potrebbe consentire attacchi Cross-Site Scripting

Richieste e risposte del test:

```
GET /conam/styles.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180
```

```
HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 179718
Keep-Alive: timeout=5, max=71
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"179718-1579614182000"
```

Date: Thu, 30 Jan 2020 14:41:08 GMT
Expires: 0
Content-Type: text/javascript

```
webpackJsonp([2],{"/node_modules/bootstrap/dist/css/bootstrap.min.css":function(e,o,t){var
r=t("./node_modules/css-loader/index.js?
{"sourceMap":false,"importLoaders":1)!./node_modules/postcss-loader/index.js?
{"ident":"postcss"}!./node_modules/bootstrap/dist/css/bootstrap.min.css');"string"==typeof r&&(r=
[[e.i,r,""]]);t("./node_modules/style-loader/addStyles.js")(r,{});r.locals&&
(e.exports=r.locals)},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.eot":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.f4769f9bdb7466be6508.eot"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.svg":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.89889688147bd7575d63.svg"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.ttf":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.e18bbf611f2a2e43afc0.ttf"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.woff":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.fa2772327f55d8198301.woff"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.woff2":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.448c34a56d699c29117a.woff2"},'./node_modules/css-loader/index.js?
{"sourceMap":false,"importLoaders":1)!./node_modules/postcss-loader/index.js?
{"ident":"postcss"}!./node_modules/bootstrap/dist/css/bootstrap.min.css':function(e,o,t){var
r=t("./node_modules/css-loader/lib/url/escape.js");o=e.exports=t("./node_modules/css-
loader/lib/css-base.js")(!1),o.push([e.i,'/*\n * Bootstrap v3.4.1 (https://getbootstrap.com/)\n
* Copyright 2011-2019 Twitter, Inc.\n * Licensed under MIT
(https://github.com/twbs/bootstrap/blob/master/LICENSE)\n */\n\n normalize.css v3.0.3 | MIT
License | github.com/necolas/normalize.css */html{font-family:sans-serif;-ms-text-size-
adjust:100%;-webkit-text-size-
adjust:100%;body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,
nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-
align:baseline}audio:not([controls]){display:none;height:0}
[hidden],template{display:none}a{background-
color:transparent;a:active,a:hover{outline:0}abbr[title]{border-bottom:none;text-
decoration:underline;-webkit-text-decoration:underline dotted;-moz-text-decoration:underline
dotted;text-decoration:underline dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-
size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-
size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-
.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{box-sizing:content-
box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-
size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflo
w:visible}button,select{text-transform:none}button,html
input[type=button],input[type=reset],input[type=submit]{-webkit-
appearance:button;cursor:pointer}button[disabled],html input[disabled]{cursor:default}button::-
moz-focus-inner,input::-moz-focus-inner{border:0;padding:0}input{line-
height:normal}input[type=checkbox],input[type=radio]{box-sizing:border-
box;padding:0}input[type=number]::-webkit-inner-spin-button,input[type=number]::-webkit-outer-
spin-button{height:auto}input[type=search]{-webkit-appearance:textfield;box-sizing:content-
box}input[type=search]::-webkit-search-cancel-button,input[type=search]::-webkit-search-
decoration{-webkit-appearance:none}fieldset{border:1px solid silver;margin:0 2px;padding:.35em
.625em
...
...
...

```

Intestazione "X-XSS-Protection" mancante o non sicura

Severità:	Bassa
Punteggio CVSS:	5,0
URL:	https://tst-secure.sistemapiemonte.it/conam/polyfills.bundle.js
Entità:	polyfills.bundle.js (Page)
Rischio:	È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.
Cause:	Programmazione o configurazione non sicura dell'applicazione Web
Fix:	Configurare il server per l'utilizzo dell'intestazione "X-XSS-Protection" con il valore '1' (abilitato)

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta X-XSS-Protection non è presente o ha un valore non sicuro, e potrebbe consentire attacchi Cross-Site Scripting

Richieste e risposte del test:

```
GET /conam/polyfills.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
_shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 162079
Keep-Alive: timeout=5, max=70
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"162079-1579614182000"
Date: Thu, 30 Jan 2020 14:41:09 GMT
Expires: 0
Content-Type: text/javascript

webpackJsonp([1],{"/node_modules/classlist.js/classList.js":function(e,o){/*! @source
http://purl.eligrey.com/github/classList.js/blob/master/classList.js */
"document"in self&&("classList"in document.createElement("_")&&
(!document.createElementNS||"classList"in
document.createElementNS("http://www.w3.org/2000/svg","g"))?function(){
"use strict";var
e=document.createElement("_");if(e.classList.add("c1","c2"),!e.classList.contains("c2")){var
o=function(e){var o=DOMTokenList.prototype[e];DOMTokenList.prototype[e]=function(e){var
s,t=arguments.length;for(s=0;s<t;s++)e=arguments[s],o.call(this,e)};o("add"),o("remove")}if(e.cl
assList.toggle("c3",!1),e.classList.contains("c3")){var
s=DOMTokenList.prototype.toggle;DOMTokenList.prototype.toggle=function(e,o){return 1 in
arguments&&!this.contains(e)==!o?o:s.call(this,e)}e=null}():function(e){
"use strict";if("Element"in e){var o=e.Element.prototype,s=Object,t=String.prototype.trim||function()
{return this.replace(/^\s+|\s+$/g,"")};n=Array.prototype.indexOf||function(e){for(var
o=0,s=this.length;o<s;o++)if(o in this&&this[o]===e)return o;return-1},r=function(e,o)
```

```

{this.name=e,this.code=DOMException[e],this.message=o},u=function(e,o){if(" "==o)throw new
r("SYNTAX_ERR","An invalid or illegal string was specified");if(/\s/.test(o))throw new
r("INVALID_CHARACTER_ERR","String contains an invalid character");return
n.call(e,o)},d=function(e){for(var o=t.call(e.getAttribute("class"))||"",s=o.split(/\s+/):
[],n=0,r=s.length;n<r;n++)this.push(s[n]);this._updateClassName=function(){
{e.setAttribute("class",this.toString())}},l=d.prototype=[],c=function(){return new
d(this)};if(r.prototype=Error.prototype,l.item=function(e){return
this[e]||null},l.contains=function(e){return e+="",~l.indexOf(this,e)},l.add=function(){var
e,o,s=arguments,s=0,t=o.length,n=!1;do{e=o[s]+""},~l.indexOf(this,e)&&
(this.push(e),n=!0)}while(++s<t);n&&this._updateClassName(),l.remove=function(){var
e,o,s=arguments,t=0,n=s.length,r=!1;do{for(es[t]+""},o=u(this,e);-
1!==o;)this.splice(o,1),r=!0,o=u(this,e)}while(++t<n);r&&this._updateClassName(),l.toggle=functi
on(e,o){e+="",var s=this.contains(e),t=s?!0!==o&&"remove":!1!==o&&"add";return t&&this[t]
(e,!0===o||!1===o?!s):l.toString=function(){return this.join(" ")},s.defineProperty({var i=
{get:c,enumerable:!0,configurable:!0};try{s.defineProperty(o,"classList",i)}catch(e){-
2146823252===e.number&&(i.enumerable=!1,s.defineProperty(o,"classList",i))}}else
s.prototype.__defineGetter__&&o.__defineGetter__("classList",c)}(self)}),"/node_modules/core-
js/es6/array.js":function(e,o,s){s("/node_modules/core-
js/modules/es6.string.iterator.js"),s("/node_modules/core-js/modules/es6.array.is-
array.js"),s("/node_modules/core-js/modules/es6.array.from.js"),s("/node_modules/core-
js/modules/es6.array.of.js"),s("/node_modules/core-
js/modules/es6.array.join.js"),s("/node_modules/core-
js/modules/es6.array.slice.js"),s("/node_modules/core-
js/modules/es6.array.sort.js"),s("/node_modules/core-js/modules/es6.array.for-
each.js"),s("/node_modules/core-js/modules/es6.array.map.js"),s("/node_modules/core-
js/modules/es6.array.filter.js"),s("/node_modules/core-
js/modules/es6.array.some.js"),s("/node_modules/core-
js/modules/es6.array.every.js"),s("/node_modules/core-
js/modules/es6.array.reduce.js"),s("/node_modules/core-js/modules/es6.array.reduce-
right.js"),s("/node_modules/core-js/modules/es6.array.index-of.js"),s("/node_modules/core-
js/modules/es6.array.last-index-of.js"),s("/node_modules/core-js/modules/es6.array.copy-
within.js"),s("/node_modules/core-js/modules/es6.array.fill.js"),s("/node_modules/core-
...
...
...

```

Problema 4 di 4

Sommario

Intestazione "X-XSS-Protection" mancante o non sicura

Severità: Bassa

Punteggio CVSS: 5,0

URL: <https://tst-secure.sistemapiemonte.it/conam/>

Entità: (Page)

Rischio: È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause: Programmazione o configurazione non sicura dell'applicazione Web

Fix: Configurare il server per l'utilizzo dell'intestazione "X-XSS-Protection" con il valore '1' (abilitato)

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta X-XSS-Protection non è presente o ha un valore non sicuro, e potrebbe consentire attacchi Cross-Site Scripting

Richieste e risposte del test:

```
GET /conam/ HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180
```

```
HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 832
Keep-Alive: timeout=5, max=53
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"832-1579614182000"
Date: Thu, 30 Jan 2020 14:41:11 GMT
content-security-policy: script-src 'self' 'unsafe-eval';
content-security-policy: script-src 'self' 'unsafe-eval';
Expires: 0
Content-Type: text/html

<!doctype html>
<html lang="it">

<head>
  <meta charset="utf-8">
  <title>conamwcl</title>
  <base href="/conam/">

  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="Content-Security-Policy" content="script-src 'self' 'unsafe-eval'; ">
  <link rel="icon" type="image/x-icon" href="favicon.ico">
</head>

<body>
  <app-root></app-root>
  <script type="text/javascript" src="/conam/inline.bundle.js"></script><script
  type="text/javascript" src="/conam/polyfills.bundle.js"></script><script type="text/javascript"
  src="/conam/scripts.bundle.js"></script><script type="text/javascript"
  src="/conam/styles.bundle.js"></script><script type="text/javascript"
  src="/conam/vendor.bundle.js"></script><script type="text/javascript"
  src="/conam/main.bundle.js"></script></body>

</html>
```

B

Intestazione HSTS (HTTP Strict-Transport-Security) mancante o non sicura 4

Sommario

Problema 1 di 4

Sommario

Intestazione HSTS (HTTP Strict-Transport-Security) mancante o non sicura

Severità:

Bassa

Punteggio CVSS: 5,0

URL:

<https://tst-secure.sistemapiemonte.it/conam>

Entità:

conam (Page)

Rischio:

È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause:

Programmazione o configurazione non sicura dell'applicazione Web

Fix:

Implementare la politica HSTS (HTTP Strict-Transport-Security) con un valore esteso di "max-age"

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta HSTS (HTTP Strict-Transport-Security) non è presente o ha un valore "max-age" insufficiente

Richieste e risposte del test:

```
GET /conam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: tst-secure.sistemapiemonte.it
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTbjtowEIavt08R%2BZ6cuiXgARINKRoJlJtJoqo3yCSTYimxU4%2Bzy759HQ4qoi2q9qJqfRmLnsM3%2F%2FzKGfLdNXTW6p1I4FsLqK19XQmkh4sJaZWgkiFHKlgNSHVO09lyQX3bpY2SWuayItYMEZTmUgRSYFuDSkE98xyeksWE7LRukDqORtlDyFsFtqmnoWYNhloKDTbXTsWfPSfd8e1WVqB3NqJ0uk6%2BE6%2FSjFhzg8YF65r8aUnOal402DgGtOQVnOolUHAfuXbSdEwsaD4hG3hg22HxfGajKEf3Zd%2BF%2Fn3J%2BsPRlvXcwXBkwhBbiARqJvSE%2BK7v9lyv5w8y74H6PnW9L8SKT3p84KLg4utt8bbHIKQfsyzuHWdcg8LDfCaATN%2BZc%2FfjjLuN0AOHutjR7S7svBgyTcNkHQXhJk5W62geJps0DJ6S0E6jNAuXszgKl6vHLLSjblOI1t7GfI%2FHZkXTa6C76%2Ffx0UyPhiKax7Li%2Baslqyr5EingGibEI85VkvPKyXpQHlWYdAvcaYuQdcMux04R2Lnc%2F6TJWZXLtKAYQydQvKwJLqyEATBZ5TlNO%2BqmYTYPF6kKrodG%2B9AkSkmsJfKnzT6FcI%2FgMvFf0L8ue%2BOHj%2FdQrtlvb%2BK%2BWhKY95v7D49317%2BjKfFAQ%3D%3D&RelayState=cookie%3A1580142121_ecaa
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 1022
Keep-Alive: timeout=5, max=99
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580142121_ecaa=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam; path=/; HttpOnly
Date: Mon, 27 Jan 2020 16:22:01 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
```

```
<html><head>
```

```
<title>302 Found</title>
```

```
</head><body>
```

```
<h1>Found</h1>
```

```
<p>The document has moved <a href="https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?">
```

```
SAMLRequest=1ZTbjtowEIavt08R%2BZ6cuiXgARINKRoJlJtJoqo3yCSTYimxU4%2Bzy759HQ4qoi2q9qJqfRmLnsM3%2F%2FzKGfLdNXTW6p1I4FsLqK19XQmkh4sJaZWgkiFHKlgNSHVO09lyQX3bpY2SWuayItYMEZTmUgRSYFuDSkE98xyeksWE7LRukDqORtlDyFsFtqmnoWYNhloKDTbXTsWfPSfd8e1WVqB3NqJ0uk6%2BE6%2FSjFhzg8YF65r8aUnOal402DgGtOQVnOolUHAfuXbSdEwsaD4hG3hg22HxfGajKEf3Zd%2BF%2Fn3J%2BsPRlvXcwXBkwhBbiARqJvSE%2BK7v9lyv5w8y74H6PnW9L8SKT3p84KLg4utt8bbHIKQfsyzuHWdcg8LDfCaATN%2BZc%2FfjjLuN0AOHutjR7S7svBgyTcNkHQXhJk5W62geJps0DJ6S0E6jNAuXszgKl6vHLLSjblOI1t7GfI%2FHZkXTa6C76%2Ffx0UyPhiKax7Li%2Baslqyr5EingGibEI85VkvPKyXpQHlWYdAvcaYuQdcMux04R2Lnc%2F6TJWZXLtKAYQydQvKwJLqyEATBZ5TlNO%2BqmYTYPF6kKrodG%2B9AkSkmsJfKnzT6FcI%2FgMvFf0L8ue%2BOHj%
```

```
2FdQrtlvb%2BK%2BWbKY95v7D49317%2BjKfAQ%3D%3D&RelayState=cookie%3A1580142121_ecaa">here</a>.  
</p>  
</body></html>
```

Problema 2 di 4

Sommario

Intestazione HSTS (HTTP Strict-Transport-Security) mancante o non sicura

Severità: **Bassa**

Punteggio CVSS: 5,0

URL: <https://tst-secure.sistemapiemonte.it/conam/inline.bundle.js>

Entità: inline.bundle.js (Page)

Rischio: È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause: Programmazione o configurazione non sicura dell'applicazione Web

Fix: Implementare la politica HSTS (HTTP Strict-Transport-Security) con un valore esteso di "max-age"

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta HSTS (HTTP Strict-Transport-Security) non è presente o ha un valore "max-age" insufficiente

Richieste e risposte del test:

```
GET /conam/inline.bundle.js HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko  
Referer: https://tst-secure.sistemapiemonte.it/conam/  
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;  
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;  
__shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;  
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;  
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)  
Connection: Keep-Alive  
Host: tst-secure.sistemapiemonte.it  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Accept-Language: en-US  
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180
```

```
HTTP/1.1 200 OK  
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT  
Connection: Keep-Alive  
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40  
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it  
Accept-Ranges: bytes  
Pragma: no-cache  
Vary: Accept-Encoding,User-Agent  
Content-Length: 1370  
Keep-Alive: timeout=5, max=88  
Cache-Control: no-cache, no-store, must-revalidate  
Strict-Transport-Security: max-age=0  
ETag: W/"1370-1579614182000"  
Date: Thu, 30 Jan 2020 14:41:07 GMT  
Expires: 0  
Content-Type: text/javascript
```

```
!function(e){function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}var r=window.webpackJsonp;window.webpackJsonp=function(t,c,u){for(var a,i,f,l=0,s=[];l<t.length;l++)i=t[l],o[i]&&s.push(o[i][0]),o[i]=0;for(a in c)Object.prototype.hasOwnProperty.call(c,a)&&(e[a]=c[a]);for(r&&r(t,c,u);s.length;)s.shift();if(u)for(l=0;l<u.length;l++)f=n(u[l]);return f;var t={},o={5:0};n.e=function(e){function r(){a.onerror=a.onload=null,clearTimeout(i);var n=o[e];0!==n&&(n&&n[1](new Error("Loading chunk "+e+" failed.")),o[e]=void 0);var t=o[e];if(0===t)return new Promise(function(e){e()});if(t)return t[2];var c=new Promise(function(n,r){t=o[e]=[n,r]});t[2]=c;var u=document.getElementsByTagName("head")[0],a=document.createElement("script");a.type="text/javascript",a.charset="utf-8",a.async=!0,a.timeout=12e4,n.nc&&a.setAttribute("nonce",n.nc),a.src=n.p+"/"+e+".chunk.js";var i=setTimeout(r,12e4);return a.onerror=a.onload=r,u.appendChild(a),c,n.m=e,n.c=t,n.d=function(e,r,t){n.o(e,r)||Object.defineProperty(e,r,{configurable:!1,enumerable:!0,get:t})},n.n=function(e){var r=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(r,"a",r),n.o=function(e,n){return Object.prototype.hasOwnProperty.call(e,n)},n.p="/conam/",n.oe=function(e){throw console.error(e,e)}({})};return c}};
```

Problema 3 di 4

[Sommaro](#)

Intestazione HSTS (HTTP Strict-Transport-Security) mancante o non sicura

Severità:	Bassa
Punteggio CVSS:	5,0
URL:	https://tst-secure.sistemapiemonte.it/conam/styles.bundle.js
Entità:	styles.bundle.js (Page)
Rischio:	È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.
Cause:	Programmazione o configurazione non sicura dell'applicazione Web
Fix:	Implementare la politica HSTS (HTTP Strict-Transport-Security) con un valore esteso di "max-age"

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta HSTS (HTTP Strict-Transport-Security) non è presente o ha un valore "max-age" insufficiente

Richieste e risposte del test:

```
GET /conam/styles.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02; XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE; _shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a; __utma=260743567.231398534.1579858881.1579858881.1579861575.2; __utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180
```

```

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 179718
Keep-Alive: timeout=5, max=71
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"179718-1579614182000"
Date: Thu, 30 Jan 2020 14:41:08 GMT
Expires: 0
Content-Type: text/javascript

webpackJsonp([2],{"/node_modules/bootstrap/dist/css/bootstrap.min.css":function(e,o,t){var
r=t('/node_modules/css-loader/index.js?
{"sourceMap":false,"importLoaders":1)!./node_modules/postcss-loader/index.js?
{"ident":"postcss"}!./node_modules/bootstrap/dist/css/bootstrap.min.css');"string"==typeof r&&(r=
[[e.i,r,""]]);t('/node_modules/style-loader/addStyles.js')(r,{});r.locals&&
(e.exports=r.locals)},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.eot":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.f4769f9bdb7466be6508.eot"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.svg":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.89889688147bd7575d63.svg"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.ttf":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.e18bbf611f2a2e43afc0.ttf"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.woff":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.fa2772327f55d8198301.woff"},"/node_modules/bootstrap/dist/fonts/glyphicons-halflings-
regular.woff2":function(e,o,t){e.exports=t.p+"glyphicons-halflings-
regular.448c34a56d699c29117a.woff2"},'/node_modules/css-loader/index.js?
{"sourceMap":false,"importLoaders":1)!./node_modules/postcss-loader/index.js?
{"ident":"postcss"}!./node_modules/bootstrap/dist/css/bootstrap.min.css':function(e,o,t){var
r=t('/node_modules/css-loader/lib/url/escape.js');o=e.exports=t('/node_modules/css-
loader/lib/css-base.js')(!!),o.push([e.i,'/*!\n * Bootstrap v3.4.1 (https://getbootstrap.com/)\n
 * Copyright 2011-2019 Twitter, Inc.\n * Licensed under MIT
(https://github.com/twbs/bootstrap/blob/master/LICENSE)\n */\n\n normalize.css v3.0.3 | MIT
License | github.com/necolas/normalize.css */html{font-family:sans-serif;-ms-text-size-
adjust:100%;-webkit-text-size-
adjust:100%;body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,
nav,section{display:block}audio,canvas,progress,video{display:inline-block;vertical-
align:baseline}audio:not([controls]){display:none;height:0}
[hidden],template{display:none}a{background-
color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:none;text-
decoration:underline;-webkit-text-decoration:underline dotted;-moz-text-decoration:underline
dotted;text-decoration:underline dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-
size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-
size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-
.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{box-sizing:content-
box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-
size:1em}input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflo
w:visible}button,select{text-transform:none}button,html
input[type=button],input[type=reset],input[type=submit]{-webkit-
appearance:button;cursor:pointer}button[disabled],html input[disabled]{cursor:default}button::-
moz-focus-inner,input::-moz-focus-inner{border:0;padding:0}input{line-
height:normal}input[type=checkbox],input[type=radio]{box-sizing:border-
box;padding:0}input[type=number]::-webkit-inner-spin-button,input[type=number]::-webkit-outer-
spin-button{height:auto}input[type=search]{-webkit-appearance:textfield;box-sizing:content-
box}input[type=search]::-webkit-search-cancel-button,input[type=search]::-webkit-search-
decoration{-webkit-appearance:none}fieldset{border:1px solid silver;margin:0 2px;padding:.35em
.625em .75em}legend{border:0;padding:0}textarea{over
...
...
...

```

Intestazione HSTS (HTTP Strict-Transport-Security) mancante o non sicura

Severità:

Bassa

Punteggio CVSS: 5,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/polyfills.bundle.js>

Entità:

polyfills.bundle.js (Page)

Rischio:

È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause:

Programmazione o configurazione non sicura dell'applicazione Web

Fix:

Implementare la politica HSTS (HTTP Strict-Transport-Security) con un valore esteso di "max-age"

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta HSTS (HTTP Strict-Transport-Security) non è presente o ha un valore "max-age" insufficiente

Richieste e risposte del test:

```
GET /conam/polyfills.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
_shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 162079
Keep-Alive: timeout=5, max=70
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"162079-1579614182000"
Date: Thu, 30 Jan 2020 14:41:09 GMT
Expires: 0
Content-Type: text/javascript

webpackJsonp([1],{"/node_modules/classlist.js/classList.js":function(e,o){/*! @source
http://purl.eligrey.com/github/classList.js/blob/master/classList.js */
"document"in self&&("classList"in document.createElement("_")&&
(!document.createElementNS||"classList"in
document.createElementNS("http://www.w3.org/2000/svg","g"))?function(){var
e=document.createElement("_");if(e.classList.add("c1","c2"),!e.classList.contains("c2")){var
o=function(e){var o=DOMTokenList.prototype[e];DOMTokenList.prototype[e]=function(e){var
s,t=arguments.length;for(s=0;s<t;s++)e=arguments[s],o.call(this,e)};o("add"),o("remove")}if(e.cl
assList.toggle("c3",!1),e.classList.contains("c3")){var
s=DOMTokenList.prototype.toggle;DOMTokenList.prototype.toggle=function(e,o){return 1 in
arguments&&!this.contains(e)==!o?s.call(this,e)}e=null}():function(e){var
strict;if("Element"in e){var o=e.Element.prototype,s=Object,t=String.prototype.trim||function()
{return this.replace(/^\s+|\s+$/g,"")},n=Array.prototype.indexOf||function(e){for(var
```

```

o=0,s=this.length;o<s;o++)if(o in this&&this[o]===e)return o;return-1},r=function(e,o)
{this.name=e,this.code=DOMException[e],this.message=o,u=function(e,o){if(" "==o)throw new
r("SYNTAX_ERR","An invalid or illegal string was specified");if(/\s/.test(o))throw new
r("INVALID_CHARACTER_ERR","String contains an invalid character");return
n.call(e,o)},d=function(e){for(var o=t.call(e.getAttribute("class"))||""),s=o?o.split(/\s+/):
[],n=0,r=s.length;n<r;n++)this.push(s[n]);this._updateClassName=function()
{e.setAttribute("class",this.toString())},l=d.prototype=[],c=function(){return new
d(this)};if(r.prototype=Error.prototype,l.item=function(e){return
this[e]||null},l.contains=function(e){return e+="",-1!==u(this,e)},l.add=function(){var
e,o,s=arguments,t=0,n=s.length,r=!1;do{e=o[s]+ "",-1!==u(this,e)&&
(this.push(e),n=!0)}while(++s<t);n&&this._updateClassName(),l.remove=function(){var
e,o,s=arguments,t=0,n=s.length,r=!1;do{for(e=s[t]+ "",o=u(this,e);-
1!==o;)this.splice(o,1),r=!0,o=u(this,e)}while(++t<n);r&&this._updateClassName(),l.toggle=functi
on(e,o){e+="";var s=this.contains(e),t=s?!0!==o&&"remove":!1!==o&&"add";return t&&this[t]
(e),!0===o||!1!==o?o:!s},l.toString=function(){return this.join(" ")},s.defineProperty({var i=
{get:c,enumerable:!0,configurable:!0};try{s.defineProperty(o,"classList",i)}catch(e){-
2146823252===e.number&&(i.enumerable=!1,s.defineProperty(o,"classList",i))}}else
s.prototype.__defineGetter__&&o.__defineGetter__("classList",c)}(self)),"./node_modules/core-
js/es6/array.js":function(e,o,s){s("./node_modules/core-
js/modules/es6.string.iterator.js"),s("./node_modules/core-js/modules/es6.array.is-
array.js"),s("./node_modules/core-js/modules/es6.array.from.js"),s("./node_modules/core-
js/modules/es6.array.of.js"),s("./node_modules/core-
js/modules/es6.array.join.js"),s("./node_modules/core-
js/modules/es6.array.slice.js"),s("./node_modules/core-
js/modules/es6.array.sort.js"),s("./node_modules/core-js/modules/es6.array.for-
each.js"),s("./node_modules/core-js/modules/es6.array.map.js"),s("./node_modules/core-
js/modules/es6.array.filter.js"),s("./node_modules/core-
js/modules/es6.array.some.js"),s("./node_modules/core-
js/modules/es6.array.every.js"),s("./node_modules/core-
js/modules/es6.array.reduce.js"),s("./node_modules/core-js/modules/es6.array.reduce-
right.js"),s("./node_modules/core-js/modules/es6.array.index-of.js"),s("./node_modules/core-
js/modules/es6.array.last-index-of.js"),s("./node_modules/core-js/modules/es6.array.copy-
within.js"),s("./node_modules/core-js/modules/es6.array.fill.js"),s("./node_modules/core-
js/modules/es6.array.find.js"),s("./node_mod
...
...
...

```

B

Manca l'attributo HttpOnly nel cookie di sessione 2

Sommario

Problema 1 di 2

Sommario

Manca l'attributo HttpOnly nel cookie di sessione

Severità:

Bassa

Punteggio CVSS: 5,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/>

Entità:

JSESSIONID (Cookie)

Rischio:

È possibile che la sessione del cliente e i cookie vengano intercettati o manipolati e potrebbero essere utilizzati per impersonare un utente legittimo, consentendo così all'aggressore di visualizzare o modificare i record dell'utente e di eseguire transazioni come se fosse tale utente.

Cause:

L'applicazione Web imposta i cookie di sessione senza l'attributo HttpOnly

Fix:

Aggiungere l'attributo 'HttpOnly' a tutti i cookie di sessione

Differenza:

Motivazione: AppScan ha rilevato che un cookie di sessione viene utilizzato senza l'attributo "HttpOnly".

Richieste e risposte del test:

```
GET /conam/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam
Cookie: __utma=32890173.1526803074.1567412775.1567412775.1567412775.1;
__shibsession_rpplivlIRUP=_802eddf8c7ca08c71757be2deb189387;
__utms=32890173.1567412775.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTzjtowFIavp08R%2BZ4sQBmwaImGSI3EkiYZVPUGOcmhWErs1MeZYd6%2BDouKaIuquaha32TxWT7%2F55f
HyKqyprNG70UM3xpAbR2qUiA9bKxIowSVDD1SwSpAgnOazJYL2rVdWiupZS5LYs0QQWkuhS8FNhWoBNQzz%2BEpXkzIXUsaqe
No1B2EvFFgm3oaKlZzqKTQYHPTlPzZc5I9zzJZgt7biNJpO3WdaJ2kxJobNC5Y2%2BRPS3JW8aLG2jGgO17CuV4MBVeQaydJ1
sQK5xOyzYb9%2FnbQ7EbgZb32PcsGxTDrPQ69fDAYDUwYYgOhQM2EnpCu23U7rtfpuanXp32Puo9fiBWd9fjARcHF1%2FviZa
cgpB%2FTNOqczrgBhcfzmQAYfWfWw481bidCjxzqakb3u7DLYMg0CeJN6AfbKF5vwnkQb5PAf4oDOWmTNFjOojBYrldpYIfpd
hFuvK35H42dq6a3QA%2B33%2BOTmVaGIpxHsuT5qzUrs%2FniK2AaJsQjzk2Rc8rZelAcjei3Azzxoy5dVzRTHVhE4sFz%2FpM
lFles0vzSHjmH3Fo3asB0UoI4%2BoyyneVvNJETm8SJV0c7YeAeKVDGBtVT6rNGvEP4BXC7%2BE%2BLP793R6tM9tHvW%2B6u
Yb6Y85f3G7tPL7vVlPP00&RelayState=cookie%3A1580395267_6d4e
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 998
Keep-Alive: timeout=5, max=82
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: __shibstate_1580395267_6d4e=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam%2F;
path=/; HttpOnly
Date: Thu, 30 Jan 2020 14:41:07 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTzjtowFIavp08R%2BZ4sQBmwaImGSI3EkiYZVPUGOcmhWErs1MeZYd6%2BDouKaIuquaha32TxWT7%2F55f
HyKqyprNG70UM3xpAbR2qUiA9bKxIowSVDD1SwSpAgnOazJYL2rVdWiupZS5LYs0QQWkuhS8FNhWoBNQzz%2BEpXkzIXUsaqe
No1B2EvFFgm3oaKlZzqKTQYHPTlPzZc5I9zzJZgt7biNJpO3WdaJ2kxJobNC5Y2%2BRPS3JW8aLG2jGgO17CuV4MBVeQaydJ1
sQK5xOyzYb9%2FnbQ7EbgZb32PcsGxTDrPQ69fDAYDUwYYgOhQM2EnpCu23U7rtfpuanXp32Puo9fiBWd9fjARcHF1%2FviZa
cgpB%2FTNOqczrgBhcfzmQAYfWfWw481bidCjxzqakb3u7DLYMg0CeJN6AfbKF5vwnkQb5PAf4oDOWmTNFjOojBYrldpYIfpd
hFuvK35H42dq6a3QA%2B33%2BOTmVaGIpxHsuT5qzUrs%2FniK2AaJsQjzk2Rc8rZelAcjei3Azzxoy5dVzRTHVhE4sFz%2FpM
lFles0vzSHjmH3Fo3asB0UoI4%2BoyyneVvNJETm8SJV0c7YeAeKVDGBtVT6rNGvEP4BXC7%2BE%2BLP793R6tM9tHvW%2B6u
Yb6Y85f3G7tPL7vVlPP00&RelayState=cookie%3A1580395267_6d4e">here</a>.</p>
</body></html>
```

Manca l'attributo HttpOnly nel cookie di sessione

Severità:

Bassa

Punteggio CVSS: 5,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/>

Entità:

XSRF-TOKEN (Cookie)

Rischio:

È possibile che la sessione del cliente e i cookie vengano intercettati o manipolati e potrebbero essere utilizzati per impersonare un utente legittimo, consentendo così all'aggressore di visualizzare o modificare i record dell'utente e di eseguire transazioni come se fosse tale utente.

Cause:

L'applicazione Web imposta i cookie di sessione senza l'attributo HttpOnly

Fix:

Aggiungere l'attributo 'HttpOnly' a tutti i cookie di sessione

Differenza:

Motivazione: AppScan ha rilevato che un cookie di sessione viene utilizzato senza l'attributo "HttpOnly".

Richieste e risposte del test:

```
GET /conam/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam
Cookie: __utma=32890173.1526803074.1567412775.1567412775.1567412775.1;
_shibsession_rpplivlIRUP= 802eddf8c7ca08c71757be2deb189387;
__utmoz=32890173.1567412775.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTLjpswFibX06dA3ofbkM7USiJRglSkXCgwUdUNMuaksQQ2tc1M%2BvYluahR2kbVLKrWgWQ%2B1%2B%2F85
xcTRdgmw2GvdzyDrz0obe3bhit8uJiiXnIsiGIKc9KCwpriPFwusG%2B7uJNCCyaoZIVKgdRM8Ehwlbcgc5DPjMJTtpiindad
wo6jlR4poL0E29TT0JKOQSu4Bptpp2HPnpPvWFWJBvTOVko4QyffSdd5gay5QWocDE3%2BtCQjLas71TkGdMsaONXLoGYSqHb
yfI2sZD5FJfHHQVB7vker8dh7S0hw%2F0iBVA8BrYLqEUyYUj0kXGnC9RT5ru%2BOXG907xZegAMPuw%2BfkZWe9HjPeM3419
viVccghT8URT06zrgBqQ7zmQA0e2PO3Y8zGTaCDxzyYke3u5DzYtAsj7NNEsVlmq03yTzOyjjyOnrLYzp08iJdhmsTL9aqI7aQ
oF8nGK833dOJcNL0Gurt%2BnxzNtDIUyTWVdaPfrLBpxEskgWiYIg85V0VOKSfrQX0wYjQscK%2BtSLQdkUwNisCeUP2TJmdV
Lt0ixgydwfY1GglhW6hBHnyGcV0qGYSUvN4EbIedmy8A3UhCvedkPqk0a8Q%2FgFcXv8T4k9j993q4y20W9b7q5ivpjzm%2F
cbus%2FPt5c949h0%3D&RelayState=cookie%3A1580395267_cc26
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 996
Keep-Alive: timeout=5, max=89
Cache-Control: private,no-store,no-cache,max-age=0
Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580395267_cc26=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam%2F;
path=/; HttpOnly
Date: Thu, 30 Jan 2020 14:41:07 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTLjpswFibX06dA3ofbkM7USiJRglSkXCgwUdUNMuaksQQ2tc1M%2BvYluahR2kbVLKrWgWQ%2B1%2B%2F85
xcTRdgmw2GvdzyDrz0obe3bhit8uJiiXnIsiGIKc9KCwpriPFwusG%2B7uJNCCyaoZIVKgdRM8Ehwlbcgc5DPjMJTtpiindad
wo6jlR4poL0E29TT0JKOQSu4Bptpp2HPnpPvWFWJBvTOVko4QyffSdd5gay5QWocDE3%2BtCQjLas71TkGdMsaONXLoGYSqHb
yfI2sZD5FJfHHQVB7vker8dh7S0hw%2F0iBVA8BrYLqEUyYUj0kXGnC9RT5ru%2BOXG907xZegAMPuw%2BfkZWe9HjPeM3419
```


viVccghT8URTo6zrgBqQ7zmQA0e2P03Y8zGTaCDxzyYke3u5DzYtAsj7NNEsVlmq03yTzOyjyOnrLYzp08iJdhmsTL9aqI7aQ
oF8nGK833dOJcNL0Gurt%2BnxzNtDIUyTwVdaPfrLBpxEskgWiYIg85V0VOKSfrQX0wYjQscK%2BtSLQdkUwNisCeUP2TJmdV
LtOixgydwfY1Gg1hW6hBHnyGCcV0qGYSUvN4EbIedmy8A3UhCVedkPqk0a8Q%2FgFcXv8T4k9j993q4y20W9b7q5ivpjzm%2F
cbus%2FPt5c949h0%3D&RelayState=cookie%3A1580395267_cc26">here.</p>
</body></html>

Problema 1 di 2

Somario

Difesa scripting tra frame mancante o non sicura - Estesa e informativa

Severità: Informazioni

Punteggio CVSS: 0,0

URL: <https://tst-secure.sistemapiemonte.it/conam>

Entità: conam (Page)

Rischio: È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili
È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.

Cause: Insecure web application programming or configuration**Fix:** Configurare il server per l'utilizzo dell'intestazione "X-Frame-Options" con il valore DENY o SAMEORIGIN

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta X-Frame-Options non è presente o ha un valore non sicuro, e potrebbe consentire attacchi Cross-Frame Scripting

Richieste e risposte del test:

```
GET /conam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: tst-secure.sistemapiemonte.it
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 302 Found
Location: https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?
SAMLRequest=1ZTLjpswFibX06dA3oeLM2lnrCQSJUhfYUeCE1XdIMecNJBApraZSd%2B%2BJhc1StuomkXVegECn8vn%2F%2
FzyWNombknYmZ3I4GsH2jj7phaaHDYmqFOCSKq5JoI2oIlhJA8Xc4Jdn7RKGS1kjZxQa1CGSxFJobsGVA7qmTN4yuYtD0m1c
TzjDYDDaxT4Np6BhracmikMOBY49X8OfDyHd9sZAlm52otvb4T9tJVXiBnZtG4oH2TPy3JacOrVreeBd3yGk71Mqi4Ama8PF8
hJ51NUOlvhW%2BMDTEepQAORmw43LAAV759wPDx%2Ft6Gad1BIrShwkwQ9rE%2F8IMBf1cEbwnGxMefkZ0e9HjPRcXF19vibY
5BmnwoinRwPOMa1D6czwag6Ru77n6scT8RcuBQFzO63YWeB4OmeZytKygu02y1TmZxVuZx9JTFbp7kRbwI0yRerJZF7CZFOU%
2FWQWn%2Fp2Pvouk10N319%2FhopqW1SGaprDn75oR1LV8iBdTABAXIuyPySjlZD6qDEa%2BgHvjRLJpgeK6VwT21JmFNDmr
cpkW1fbQGwxfolEftoUK1MFnhDLC%2Bmo2IbWvF6mqfbsbW01AVigrdSmVOGvOK4R%2FA5eI%2FI408h%2BXH2%2Bh3bLeX8V
8NeUx7zd2n553Ly%2Fj6Xc%3D&RelayState=cookie%3A1580142122_a752
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Content-Length: 1002
Keep-Alive: timeout=5, max=67
Cache-Control: private,no-store,no-cache,max-age=0
```

```

Strict-Transport-Security: max-age=0
Set-Cookie: _shibstate_1580142122_a752=https%3A%2F%2Ftst-secure.sistemapiemonte.it%2Fconam;
path=/; HttpOnly
Date: Mon, 27 Jan 2020 16:22:02 GMT
Expires: Wed, 01 Jan 1997 12:00:00 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://tst-secure.sistemapiemonte.it/iamidpsp/profile/SAML2/Redirect/SSO?SAMLRequest=1ZTLjpswFibX06dA3oeLM2lnrCQsJUhFyoUCE1XdIMecNjbApraZsd%2B%2BJhc1StuomkXVegECn8vn%2F%2FzyWN0mbknYmZ3I4GsH2jj7phaaHDYmqFOCSKq5JoI2oIlhJA8xc4Jdn7RKGS1kjZxQa1CGSxFJobsGVA7qmTN4yuYtTD0mlcTzjDYDDaxT4Np6BhracmikMOBy49X8OfDyHd9sZA1m52otvb4T9tJVXiBnZtG4oH2TPy3JacOrVreeBd3yGk71Mqi4Ama8PF8hJ5lNUOlvhv%2BMDTEePQAORmw43LAAV759wPDx%2Ft6Gad1BIRShwkwQ9rE%2F8IMBf1cEbwnGxmefkZoe9HjPRcXF19vibY5BmnwoinRwPOMalD6czwag6Ru77n6sct8RcuBQFzO63YWeB4OmeZytkygu02y1TmZxVuZx9JTFbp7kRbwI0yRerJZF7CZFOU%2FWQWn%2Fp2Pvouk10N319%2FhopqW1SGaprDn75oR1LV8iBdTABAXIuyppySjlZD6qDEaN%2BgHvjRLJpgeK6VwT21JmfNDmrCpkWlfbQGwxfo1EftoUK1MFnhDLC%2Bmo2IbWvF6mqfsbWO1AVigrdSmVOGv0K4R%2FA5eI%2FI408h%2BHX2%2Bh3bLeX8V8NeUx7zd2n553Ly%2Fj6Xc%3D&RelayState=cookie%3A1580142122_a752">here</a>.</p>
</body></html>

```

Problema 2 di 2

[Sommaro](#)

Difesa scripting tra frame mancante o non sicura - Estesa e informativa

Severità:	Informazioni
Punteggio CVSS:	0,0
URL:	https://tst-secure.sistemapiemonte.it/conam/
Entità:	(Page)
Rischio:	È possibile raccogliere informazioni sensibili sull'applicazione Web come nomi utente, password, nome macchina e/o posizioni dei file sensibili È possibile persuadere un utente ingenuo a fornire informazioni sensibili, ad esempio nome utente, password, numero di carta di credito, numero della previdenza sociale, ecc.
Cause:	Insecure web application programming or configuration
Fix:	Configurare il server per l'utilizzo dell'intestazione "X-Frame-Options" con il valore DENY o SAMEORIGIN

Differenza:

Motivazione: AppScan ha rilevato che l'intestazione della risposta X-Frame-Options non è presente o ha un valore non sicuro, e potrebbe consentire attacchi Cross-Frame Scripting

Richieste e risposte del test:

```

GET /conam/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXfy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
_shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utms=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

```

```
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 832
Keep-Alive: timeout=5, max=53
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"832-1579614182000"
Date: Thu, 30 Jan 2020 14:41:11 GMT
content-security-policy: script-src 'self' 'unsafe-eval';
content-security-policy: script-src 'self' 'unsafe-eval';
Expires: 0
Content-Type: text/html

<!doctype html>
<html lang="it">

<head>
  <meta charset="utf-8">
  <title>conamwcl</title>
  <base href="/conam/">

  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="Content-Security-Policy" content="script-src 'self' 'unsafe-eval'; ">
  <link rel="icon" type="image/x-icon" href="favicon.ico">
</head>

<body>
  <app-root></app-root>
  <script type="text/javascript" src="/conam/inline.bundle.js"></script><script
  type="text/javascript" src="/conam/polyfills.bundle.js"></script><script type="text/javascript"
  src="/conam/scripts.bundle.js"></script><script type="text/javascript"
  src="/conam/styles.bundle.js"></script><script type="text/javascript"
  src="/conam/vendor.bundle.js"></script><script type="text/javascript"
  src="/conam/main.bundle.js"></script></body>

</html>
```

Individuazione di possibile pattern di divulgazione percorso server

Severità:

Informazioni

Punteggio CVSS: 0,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/styles.bundle.js>

Entità:

styles.bundle.js (Page)

Rischio:

È possibile richiamare il percorso assoluto di installazione del server Web, che potrebbe essere utile ad un aggressore per sviluppare altri attacchi ed ottenere informazioni sulla struttura del file system dell'applicazione Web

Cause:

Non sono state installate le patch o gli hotfix più recenti per i prodotti di terze parti.

Fix:

Scaricare la patch di sicurezza pertinente per il server Web o l'applicazione Web.

Differenza:

Motivazione: La risposta contiene i percorsi assoluti e/o nomi file di file presenti sul server.

Richieste e risposte del test:

```
GET /conam/styles.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=fqfrW226yNzsuRFmMHZbTXFy.jb6part219conam_tunode02;
XSRF-TOKEN=-6599009836272156781-5505324362561319180; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliv1SISP=_3d0af24ffa25762b38aaaae75921643a;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: -6599009836272156781-5505324362561319180

...
...
...lfings";src:url('+(t("./node_modules/bootstrap/dist/fonts/glyphicons-halflings-regular.eot"))+');src:url('+(t("./node_modules/bootstrap/dist/fonts/glyphicons-halflings-regular.eot"))+'?#iefix) format("embedded-opentype"),url('+(t("./node_modules/bootstrap/dist/fonts/glyphicons-halflings-regular.woff2"))+' format("woff2"),url('+(t("./node_modules/bootstrap/dist/fonts/glyphicons-halflings-regular.woff"))+') format("woff"),url('+(t("./node_modules/bootstrap/dist/fonts/glyphicons-halflings-regular.ttf"))+') format("truetype"),url('+(t("./node_modules/bootstrap/dist/fonts/glyphicons-halflings-regular.svg"))+'#glyphicons_halflingsregular) format("svg")}.glyphicon{position:relative;top:1px;display:inline-block;font-family:"Glyphicons Halflings";font-style:normal;font-weight:400;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.glyphicon-asterisk:before{content:"*"}.glyphicon-plus:before{content:"+"}.glyphicon-eur:before,.glyphicon-euro:before{content:"\20AC"}.glyphicon-minus:before{content:"\2212"}.glyphicon-cloud:before{content:"\2601"}.glyphicon-envelope:before{content:"\2709"}.glyphicon-pencil:before{content:"\270F"}.glyphicon-glass:before{content:"\E001"}.glyphicon-music:before{content:"\E002"}.glyphicon-search:before{content:"\E003"}.glyphicon-heart:before{content:"\E005"}.glyphicon-star:before{content:"\E006"}.glyphicon-star-empty:before{content:"\E007"}.glyphicon-user:before{content:"\E008"}.glyphicon-film:before{content:"\E009"}.glyphicon-th-large:before{content:"\E010"}.glyphicon-th:before{content:"\E011"}.glyphicon-th-list:before{content:"\E012"}.glyphicon-ok:before{content:"\E013"}.glyphicon-remove:before{content:"\E014"}.glyphicon-zoom-in:before{content:"\E015"}.glyphicon-zoom-out:before{content:"\E016"}.glyphicon-off:before{content:"\E017"}.glyphicon-signal:before{content:"\E018"}.glyphicon-cog:before{content:"\E019"}.glyphicon-trash:before{content:"\E020"}.glyphicon-home:before{content:"\E021"}.glyphicon-file:before{content:"\E022"}.glyphicon-time:before{content:"\E023"}.glyphicon-road:before{content:"\E024"}.glyphicon-download-alt:before{content:"\E025"}.glyphicon-download:before{content:"\E026"}.glyphicon-upload:before{content:"\E027"}.glyphicon-inbox:before{content:"\E028"}.glyphicon-play-circle:before{content:"\E029"}.glyphicon-repeat:before{content:"\E030"}.glyphicon-refresh:before{content:"\E031"}.glyphicon-list-alt:before{content:"\E032"}.glyphicon-lock:before{content:"\E033"}.glyphicon-flag:before{content:"\E034"}.glyphicon-headphones:before{content:"\E035"}.glyphicon-volume-
```

off:before{content:"\E036"}.glyphicon-volume-down:before{content:"\E037"}.glyphicon-volume-up:before{content:"\E038"}.glyphicon-qr-code:before{content:"\E039"}.glyphicon-barcode:before{content:"\E040"}.glyphicon-tag:before{content:"\E041"}.glyphicon-tags:before{content:"\E042"}.glyphicon-book:before{content:"\E043"}.glyphicon-bookmark:before{content:"\E044"}.glyphicon-print:before{content:"\E045"}.glyphicon-camera:before{content:"\E046"}.glyphicon-font:before{content:"\E047"}.glyphicon-bold:before{content:"\E048"}.glyphicon-italic:before{content:"\E049"}.glyphicon-text-height:before{content:"\E050"}.glyphicon-text-width:before{content:"\E051"}.glyphicon-align-left:before{content:"\E052"}.glyphicon-align-center:before{content:"\E053"}.glyphicon-align-right:before{content:"\E054"}.glyphicon-align-justify:before{content:"\E055"}.glyphicon-list:before{content:"\E056"}.glyphicon-indent-left:before{content:"\E057"}.glyphicon-indent-right:before{content:"\E058"}.glyphicon-facetime-video:before{content:"\E059"}.glyphicon-picture:before{content:"\E060"}.glyphicon-map-marker:before{content:"\E062"}.glyphicon-adjust:before{content:"\E063"}.glyphicon-tint:before{content:"\E064"}.glyphicon-edit:before{content:"\E065"}.glyphicon-share:before{content:"\E066"}.glyphicon-check:before{content:"\E067"}.glyphicon-move:before{content:"\E068"}.glyphicon-step-backward:before{content:"\E069"}.glyphicon-fast-backward:before{content:"\E070"}.glyphicon-backward:before{content:"\E071"}.glyphicon-play:before{content:"\E072"}.glyphicon-pause:before{content:"\E073"}.glyphicon-stop:before{content:"\E074"}.glyphicon-forward:before{content:"\E075"}.glyphicon-fast-forward:before{content:"\E076"}.glyphicon-step-forward:before{content:"\E077"}.glyphicon-eject:before{content:"\E078"}.glyphicon-chevron-left:before{content:"\E079"}.glyphicon-chevron-right:before{content:"\E080"}.glyphicon-plus-sign:before{content:"\E081"}.glyphicon-minus-sign:before{content:"\E082"}.glyphicon-remove-sign:before{content:"\E083"}.glyphicon-ok-sign:before{content:"\E084"}.glyphicon-question-sign:before{content:"\E085"}.glyphicon-info-sign:before{content:"\E086"}.glyphicon-screenshot:before{content:"\E087"}.glyphicon-remove-circle:before{content:"\E088"}.glyphicon-ok-circle:before{content:"\E089"}.glyphicon-ban-circle:before{content:"\E090"}.glyphicon-arrow-left:before{content:"\E091"}.glyphicon-arrow-right:before{content:"\E092"}.glyphicon-arrow-up:before{content:"\E093"}.glyphicon-arrow-down:before{content:"\E094"}.glyphicon-share-alt:before{content:"\E095"}.glyphicon-resize-full:before{content:"\E096"}.glyphicon-resize-small:before{content:"\E097"}.glyphicon-exclamation-sign:before{content:"\E101"}.glyphicon-gift:before{content:"\E102"}.glyphicon-leaf:before{content:"\E103"}.glyphicon-fire:before{content:"\E104"}.glyphicon-eye-open:before{content:"\E105"}.glyphicon-eye-close:before{content:"\E106"}.glyphicon-warning-sign:before{content:"\E107"}.glyphicon-plane:before{content:"\E108"}.glyphicon-calendar:before{content:"\E109"}.glyphicon-random:before{content:"\E110"}.glyphicon-comment:before{content:"\E111"}.glyphicon-magnet:before{content:"\E112"}.glyphicon-chevron-up:before{content:"\E113"}.glyphicon-chevron-down:before{content:"\E114"}.glyphicon-retweet:before{content:"\E115"}.glyphicon-shopping-cart:before{content:"\E116"}.glyphicon-folder-close:before{content:"\E117"}.glyphicon-folder-open:before{content:"\E118"}.glyphicon-resize-vertical:before{content:"\E119"}.glyphicon-resize-horizontal:before{content:"\E120"}.glyphicon-hdd:before{content:"\E121"}.glyphicon-bullhorn:before{content:"\E122"}.glyphicon-bell:before{content:"\E123"}.glyphicon-certificate:before{content:"\E124"}.glyphicon-thumbs-up:before{content:"\E125"}.glyphicon-thumbs-down:before{content:"\E126"}.glyphicon-hand-right:before{content:"\E127"}.glyphicon-hand-left:before{content:"\E128"}.glyphicon-hand-up:before{content:"\E129"}.glyphicon-hand-down:before{content:"\E130"}.glyphicon-circle-arrow-right:before{content:"\E131"}.glyphicon-circle-arrow-left:before{content:"\E132"}.glyphicon-circle-arrow-up:before{content:"\E133"}.glyphicon-circle-arrow-down:before{content:"\E134"}.glyphicon-globe:before{content:"\E135"}.glyphicon-wrench:before{content:"\E136"}.glyphicon-tasks:before{content:"\E137"}.glyphicon-filter:before{content:"\E138"}.glyphicon-briefcase:before{content:"\E139"}.glyphicon-fullscreen:before{content:"\E140"}.glyphicon-dashboard:before{content:"\E141"}.glyphicon-paperclip:before{content:"\E142"}.glyphicon-heart-empty:before{content:"\E143"}.glyphicon-link:before{content:"\E144"}.glyphicon-phone:before{content:"\E145"}.glyphicon-pushpin:before{content:"\E146"}.glyphicon-usd:before{content:"\E148"}.glyphicon-gbp:before{content:"\E149"}.glyphicon-sort:before{content:"\E150"}.glyphicon-sort-by-alphabet:before{content:"\E151"}.glyphicon-sort-by-alphabet-alt:before{content:"\E152"}.glyphicon-sort-by-order:before{content:"\E153"}.glyphicon-sort-by-order-alt:before{content:"\E154"}.glyphicon-sort-by-attributes:before{content:"\E155"}.glyphicon-sort-by-attributes-alt:before{content:"\E156"}.glyphicon-unchecked:before{content:"\E157"}.glyphicon-expand:before{content:"\E158"}.glyphicon-collapse-down:before{content:"\E159"}.glyphicon-collapse-up:before{content:"\E160"}.glyphicon-log-in:before{content:"\E161"}.glyphicon-flash:before{content:"\E162"}.glyphicon-log-out:before{content:"\E163"}.glyphicon-new-window:before{content:"\E164"}.glyphicon-record:before{content:"\E165"}.glyphicon-save:before{content:"\E166"}.glyphicon-open:before{content:"\E167"}.glyphicon-saved:before{content:"\E168"}.glyphicon-import:before{content:"\E169"}.glyphicon-export:before{content:"\E170"}.glyphicon-send:before{content:"\E171"}.glyphicon-floppy-disk:before{content:"\E172"}.glyphicon-floppy-saved:before{content:"\E173"}.glyphicon-floppy-remove:before{content:"\E174"}.glyphicon-floppy-save:before{content:"\E175"}.glyphicon-floppy-open:before{content:"\E176"}.glyphicon-credit-card:before{content:"\E177"}.glyphicon-transfer:before{content:"\E178"}.glyphicon-cutlery:before{content:"\E179"}.glyphicon-header:before{content:"\E180"}.glyphicon-compressed:before{content:"\E181"}.glyphicon-earphone:before{content:"\E182"}.glyphicon-phone-alt:before{content:"\E183"}.glyphicon-tower:before{content:"\E184"}.glyphicon-stats:before{content:"\E185"}.glyphicon-sd-video:before{content:"\E186"}.glyphicon-hd-video:before{content:"\E187"}.glyphicon-subtitles:before{content:"\E188"}.glyphicon-sound-stereo:before{content:"\E189"}.glyphicon-sound-dolby:before{content:"\E190"}.glyphicon-sound-5-1:before{content:"\E191"}.glyphicon-sound-6-1:before{content:"\E192"}.glyphicon-sound-7-1:before{content:"\E193"}.glyphicon-

```

copyright-mark:before{content:"\E194"}.glyphicon-registration-
mark:before{content:"\E195"}.glyphicon-cloud-download:before{content:"\E197"}.glyphicon-cloud-
upload:before{content:"\E198"}.glyphicon-tree-conifer:before{content:"\E199"}.glyphicon-tree-
deciduous:before{content:"\E200"}.glyphicon-cd:before{content:"\E201"}.glyphicon-save-
file:before{content:"\E202"}.glyphicon-open-file:before{content:"\E203"}.glyphicon-level-
up:before{content:"\E204"}.glyphicon-copy:before{content:"\E205"}.glyphicon-
paste:before{content:"\E206"}.glyphicon-alert:before{content:"\E209"}.glyphicon-
equalizer:before{content:"\E210"}.glyphicon-king:before{content:"\E211"}.glyphicon-
queen:before{content:"\E212"}.glyphicon-pawn:before{content:"\E213"}.glyphicon-
bishop:before{content:"\E214"}.glyphicon-knight:before{content:"\E215"}.glyphicon-baby-
formula:before{content:"\E216"}.glyphicon-tent:before{content:"\E26FA"}.glyphicon-
blackboard:before{content:"\E218"}.glyphicon-bed:before{content:"\E219"}.glyphicon-
apple:before{content:"\F8FF"}.glyphicon-erase:before{content:"\E221"}.glyphicon-
hourglass:before{content:"\E231B"}.glyphicon-lamp:before{content:"\E223"}.glyphicon-
duplicate:before{content:"\E224"}.glyphicon-piggy-bank:before{content:"\E225"}.glyphicon-
scissors:before{content:"\E226"}.glyphicon-bitcoin:before{content:"\E227"}.glyphicon-
btc:before{content:"\E227"}.glyphicon-xbt:before{content:"\E227"}.glyphicon-
yen:before{content:"\A5"}.glyphicon-jpy:before{content:"\A5"}.glyphicon-
ruble:before{content:"\E20BD"}.glyphicon-rub:before{content:"\E20BD"}.glyphicon-
scale:before{content:"\E230"}.glyphicon-ice-lolly:before{content:"\E231"}.glyphicon-ice-lolly-
tasted:before{content:"\E232"}.glyphicon-education:before{content:"\E233"}.glyphicon-option-
horizontal:before{content:"\E234"}.glyphicon-option-vertical:before{content:"\E235"}.glyphicon-
menu-hamburger:before{content:"\E236"}.glyphicon-modal-
window:before{content:"\E237"}.glyphicon-oil:before{content:"\E238"}.glyphicon-
grain:before{content:"\E239"}.glyphicon-sunglasses:before{content:"\E240"}.glyphicon-text-
size:before{content:"\E241"}.glyphicon-text-color:before{content:"\E242"}.glyphicon-text-
background:before{content:"\E243"}.glyphicon-object-align-
top:before{content:"\E244"}.glyphicon-object-align-bottom:before{content:"\E245"}.glyphicon-
object-align-horizontal:before{content:"\E246"}.glyphicon-object-align-
left:before{content:"\E247"}.glyphicon-object-align-vertical:before{content:"\E248"}.glyphicon-
object-align-right:before{content:"\E249"}.glyphicon-triangle-
right:before{content:"\E250"}.glyphicon-triangle-left:before{content:"\E251"}.glyphicon-
triangle-bottom:before{content:"\E252"}.glyphicon-triangle-
top:before{content:"\E253"}.glyphicon-console:before{content:"\E254"}.glyphicon-
superscript:before{content:"\E255"}.glyphicon-subscript:before{content:"\E256"}.glyphicon-menu-
left:before{content:"\E257"}.glyphicon-menu-right:before{content:"\E258"}.glyphicon-menu-
down:before{content:"\E259"}.glyphicon-menu-up:before{content:"\E260"}*{box-sizing:border-
box}:after,:before{box-sizing:border-box}html{font-size:10px;-webkit-tap-highlight-
color:rgba(0,0,0,0)}body{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;font-
size:14px;line-height:1.42857143;color:#333;background-
color:#fff}button,input,select,textarea{font-family:inherit;font-size:inherit;line-
height:inherit}a{color:#337ab7;text-decoration:none}a:focus,a:hover{color:#23527c;text-
decoration:underline}a:focus{outline:5px auto -webkit-focus-ring-color;outline-offset:-
2px}figure{margin:0}img{vertical-align:middle}.carousel-inner>.item>a>img,.carousel-
inner>.item>img,.img-responsive,.thumbnail a>img,.thumbnail>img{display:block;max-
width:100%;height:auto}.img-rounded{border-radius:6px}.img-thumbnail{padding:4px;line-
height:1.42857143;background-color:#fff;border:1px solid #ddd;border-radius:4px;transition:all
.2s ease-in-out;display:inline-block;max-width:100%;height:auto}.img-circle{border-
radius:50%}hr{ma
...
...
...
in-bottom:10px}ol ol,ol ul,ul ol,ul ul{margin-bottom:0}.list-unstyled{padding-left:0;list-
style:none}.list-inline{padding-left:0;list-style:none;margin-left:-5px}.list-
inline>li{display:inline-block;padding-right:5px;padding-left:5px}dl{margin-top:0;margin-
bottom:20px}dd,dt{line-height:1.42857143}dt{font-weight:700}dd{margin-left:0}@media (min-
width:768px){.dl-horizontal dt{float:left;width:160px;clear:left;text-
align:right;overflow:hidden;text-overflow:ellipsis;white-space:nowrap}.dl-horizontal dd{margin-
left:180px}abbr[data-original-title],abbr[title]{cursor:help}.initialism{font-size:90%;text-
transform:uppercase}blockquote{padding:10px 20px;margin:0 0 20px;font-size:17.5px;border-left:5px
solid #eee}blockquote ol:last-child,blockquote p:last-child,blockquote ul:last-child{margin-
bottom:0}blockquote .small,blockquote footer,blockquote small{display:block;font-size:80%;line-
height:1.42857143;color:#777}blockquote .small:before,blockquote footer:before,blockquote
small:before{content:"\2014 \A0"}.blockquote-reverse,blockquote.pull-right{padding-
right:15px;padding-left:0;text-align:right;border-right:5px solid #eee;border-left:0}.blockquote-
reverse .small:before,.blockquote-reverse footer:before,.blockquote-reverse
small:before,blockquote.pull-right .small:before,blockquote.pull-right
footer:before,blockquote.pull-right small:before{content:""}.blockquote-reverse
.small:after,.blockquote-reverse footer:after,.blockquote-reverse small:after,blockquote.pull-
right .small:after,blockquote.pull-right footer:after,blockquote.pull-right
small:after{content:"\A0 \2014"}address{margin-bottom:20px;font-style:normal;line-
height:1.42857143}code,kbd,pre,samp{font-family:Menlo,Monaco,Consolas,"Courier
New",monospace}code{padding:2px 4px;font-size:90%;color:#c7254e;background-color:#f9f2f4;border-
radius:4px}kbd{padding:2px 4px;font-size:90%;color:#fff;background-color:#333;border-
radius:3px;box-shadow:inset 0 -1px 0 rgba(0,0,0,.25)}kbd kbd{padding:0;font-size:100%;font-
weight:700;box-shadow:none}pre{display:block;padding:9.5px;margin:0 0 10px;font-size:13px;line-
height:1.42857143;color:#333;word-break:break-all;word-wrap:break-word;background-
color:#f5f5f5;border:1px solid #ccc;border-radius:4px}pre code{padding:0;font-

```

```

size:inherit;color:inherit;white-space:pre-wrap;background-color:transparent;border-
radius:0}.pre-scrollable{max-height:340px;overflow-y:scroll}.container{padding-
right:15px;padding-left:15px;margin-right:auto;margin-left:auto}@media (min-width:768px)
{.container{width:750px}}@media (min-wid
...
...
...
background-repeat:repeat-x}.carousel-control.right{right:0;left:auto;background-image:linear-
gradient(to right,rgba(0,0,0,.0001) 0,rgba(0,0,0,.5)
100%);filter:progid:DXImageTransform.Microsoft.gradient(startColorstr=\'#00000000\',
endColorstr=\'#80000000\', GradientType=1);background-repeat:repeat-x}.carousel-
control:focus,.carousel-control:hover{color:#fff;text-
decoration:none;outline:0;filter:alpha(opacity=90);opacity:.9}.carousel-control .glyphicon-
chevron-left,.carousel-control .glyphicon-chevron-right,.carousel-control .icon-next,.carousel-
control .icon-prev{position:absolute;top:50%;z-index:5;display:inline-block;margin-top:-
10px}.carousel-control .glyphicon-chevron-left,.carousel-control .icon-prev{left:50%;margin-
left:-10px}.carousel-control .glyphicon-chevron-right,.carousel-control .icon-
next{right:50%;margin-right:-10px}.carousel-control .icon-next,.carousel-control .icon-
prev{width:20px;height:20px;font-family:serif;line-height:1}.carousel-control .icon-
prev:before{content:"\2039"}.carousel-control .icon-next:before{content:"\203A"}.carousel-
indicators{position:absolute;bottom:10px;left:50%;z-index:15;width:60%;padding-left:0;margin-
left:-30%;text-align:center;list-style:none}.carousel-indicators li{display:inline-
block;width:10px;height:10px;margin:1px;text-indent:-999px;cursor:pointer;background-
color:#000\9;background-color:rgba(0,0,0,0);border:1px solid #fff;border-radius:10px}.carousel-
indicators .active{width:12px;height:12px;margin:0;background-color:#fff}.carousel-
caption{position:absolute;right:15%;bottom:20px;left:15%;z-index:10;padding-top:20px;padding-
bottom:20px;color:#fff;text-align:center;text-shadow:0 1px 2px rgba(0,0,0,.6)}.carousel-caption
.btn{text-shadow:none}@media screen and (min-width:768px){.carousel-control .glyphicon-chevron-
left,.carousel-control .glyphicon-chevron-right,.carousel-control .icon-next,.carousel-control
.icon-prev{width:30px;height:30px;margin-top:-10px;font-size:30px}.carousel-control .glyphicon-
chevron-left,.carousel-
...
...
...
59deg)}}.fa-rotate-90{-ms-
filter:"progid:DXImageTransform.Microsoft.BasicImage(rotation=1)";transform:rotate(90deg)}.fa-
rotate-180{-ms-
filter:"progid:DXImageTransform.Microsoft.BasicImage(rotation=2)";transform:rotate(180deg)}.fa-
rotate-270{-ms-
filter:"progid:DXImageTransform.Microsoft.BasicImage(rotation=3)";transform:rotate(270deg)}.fa-
flip-horizontal{-ms-filter:"progid:DXImageTransform.Microsoft.BasicImage(rotation=0,
mirror=1)";transform:scale(-1, 1)}.fa-flip-vertical{-ms-
filter:"progid:DXImageTransform.Microsoft.BasicImage(rotation=2, mirror=1)";transform:scale(1, -
1)}.root .fa-rotate-90,.root .fa-rotate-180,.root .fa-rotate-270,.root .fa-flip-horizontal,.root
.fla-flip-vertical{filter:none}.fa-stack{position:relative;display:inline-
block;width:2em;height:2em;line-height:2em;vertical-align:middle}.fa-stack-1x,.fa-stack-
2x{position:absolute;left:0;width:100%;text-align:center}.fa-stack-1x{line-height:inherit}.fa-
stack-2x{font-size:2em}.fa-inverse{color:#fff}.fa-glass:before{content:"\F000"}.fa-
music:before{content:"\F001"}.fa-search:before{content:"\F002"}.fa-envelope-
o:before{content:"\F003"}.fa-heart:before{content:"\F004"}.fa-star:before{content:"\F005"}.fa-
star-o:before{content:"\F006"}.fa-user:before{content:"\F007"}.fa-
film:before{content:"\F008"}.fa-th-large:before{content:"\F009"}.fa-
th:before{content:"\F00A"}.fa-th-list:before{content:"\F00B"}.fa-
check:before{content:"\F00C"}.fa-remove:before,.fa-close:before,.fa-
times:before{content:"\F00D"}.fa-search-plus:before{content:"\F00E"}.fa-search-
minus:before{content:"\F010"}.fa-power-off:before{content:"\F011"}.fa-
signal:before{content:"\F012"}.fa-gear:before,.fa-cog:before{content:"\F013"}.fa-trash-
o:before{content:"\F014"}.fa-home:before{content:"\F015"}.fa-file-
o:before{content:"\F016"}.fa-clock-o:before{content:"\F017"}.fa-
road:before{content:"\F018"}.fa-download:before{content:"\F019"}.fa-arrow-circle-o-
down:before{content:"\F01A"}.fa-arrow-circle-o-up:before{content:"\F01B"}.fa-
inbox:before{content:"\F01C"}.fa-play-circle-o:before{content:"\F01D"}.fa-rotate-
right:before,.fa-repeat:before{content:"\F01E"}.fa-refresh:before{content:"\F021"}.fa-list-
alt:before{content:"\F022"}.fa-lock:before{content:"\F023"}.fa-
flag:before{content:"\F024"}.fa-headphones:before{content:"\F025"}.fa-volume-
off:before{content:"\F026"}.fa-volume-down:before{content:"\F027"}.fa-volume-
up:before{content:"\F028"}.fa-qrcode:before{content:"\F029"}.fa-
barcode:before{content:"\F02A"}.fa-tag:before{content:"\F02B"}.fa-
tags:before{content:"\F02C"}.fa-book:before{content:"\F02D"}.fa-
bookmark:before{content:"\F02E"}.fa-print:before{content:"\F02F"}.fa-
camera:before{content:"\F030"}.fa-font:before{content:"\F031"}.fa-
bold:before{content:"\F032"}.fa-italic:before{content:"\F033"}.fa-text-
height:before{content:"\F034"}.fa-text-width:before{content:"\F035"}.fa-align-
left:before{content:"\F036"}.fa-align-center:before{content:"\F037"}.fa-align-
right:before{content:"\F038"}.fa-align-justify:before{content:"\F039"}.fa-
list:before{content:"\F03A"}.fa-dedent:before,.fa-outdent:before{content:"\F03B"}.fa-
indent:before{content:"\F03C"}.fa-video-camera:before{content:"\F03D"}.fa-photo:before,.fa-
image:before,.fa-picture-o:before{content:"\F03E"}.fa-pencil:before{content:"\F040"}.fa-map-

```



```

marker:before{content:"\F041"}.fa-adjust:before{content:"\F042"}.fa-
tint:before{content:"\F043"}.fa-edit:before,.fa-pencil-square-o:before{content:"\F044"}.fa-
share-square-o:before{content:"\F045"}.fa-check-square-o:before{content:"\F046"}.fa-
arrows:before{content:"\F047"}.fa-step-backward:before{content:"\F048"}.fa-fast-
backward:before{content:"\F049"}.fa-backward:before{content:"\F04A"}.fa-
play:before{content:"\F04B"}.fa-pause:before{content:"\F04C"}.fa-
stop:before{content:"\F04D"}.fa-forward:before{content:"\F04E"}.fa-fast-
forward:before{content:"\F050"}.fa-step-forward:before{content:"\F051"}.fa-
eject:before{content:"\F052"}.fa-chevron-left:before{content:"\F053"}.fa-chevron-
right:before{content:"\F054"}.fa-plus-circle:before{content:"\F055"}.fa-minus-
circle:before{content:"\F056"}.fa-times-circle:before{content:"\F057"}.fa-check-
circle:before{content:"\F058"}.fa-question-circle:before{content:"\F059"}.fa-info-
circle:before{content:"\F05A"}.fa-crosshairs:before{content:"\F05B"}.fa-times-circle-
o:before{content:"\F05C"}.fa-check-circle-o:before{content:"\F05D"}.fa-
ban:before{content:"\F05E"}.fa-arrow-left:before{content:"\F060"}.fa-arrow-
right:before{content:"\F061"}.fa-arrow-up:before{content:"\F062"}.fa-arrow-
down:before{content:"\F063"}.fa-mail-forward:before,.fa-share:before{content:"\F064"}.fa-
expand:before{content:"\F065"}.fa-compress:before{content:"\F066"}.fa-
plus:before{content:"\F067"}.fa-minus:before{content:"\F068"}.fa-
asterisk:before{content:"\F069"}.fa-exclamation-circle:before{content:"\F06A"}.fa-
gift:before{content:"\F06B"}.fa-leaf:before{content:"\F06C"}.fa-
fire:before{content:"\F06D"}.fa-eye:before{content:"\F06E"}.fa-eye-
slash:before{content:"\F070"}.fa-warning:before,.fa-exclamation-
triangle:before{content:"\F071"}.fa-plane:before{content:"\F072"}.fa-
calendar:before{content:"\F073"}.fa-random:before{content:"\F074"}.fa-
comment:before{content:"\F075"}.fa-magnet:before{content:"\F076"}.fa-chevron-
up:before{content:"\F077"}.fa-chevron-down:before{content:"\F078"}.fa-
retweet:before{content:"\F079"}.fa-shopping-cart:before{content:"\F07A"}.fa-
folder:before{content:"\F07B"}.fa-folder-open:before{content:"\F07C"}.fa-arrows-
v:before{content:"\F07D"}.fa-arrows-h:before{content:"\F07E"}.fa-bar-chart-o:before,.fa-bar-
chart:before{content:"\F080"}.fa-twitter-square:before{content:"\F081"}.fa-facebook-
square:before{content:"\F082"}.fa-camera-retro:before{content:"\F083"}.fa-
key:before{content:"\F084"}.fa-gears:before,.fa-cogs:before{content:"\F085"}.fa-
comments:before{content:"\F086"}.fa-thumbs-o-up:before{content:"\F087"}.fa-thumbs-o-
down:before{content:"\F088"}.fa-star-half:before{content:"\F089"}.fa-heart-
o:before{content:"\F08A"}.fa-sign-out:before{content:"\F08B"}.fa-linkedin-
square:before{content:"\F08C"}.fa-thumb-tack:before{content:"\F08D"}.fa-external-
link:before{content:"\F08E"}.fa-sign-in:before{content:"\F090"}.fa-
trophy:before{content:"\F091"}.fa-github-square:before{content:"\F092"}.fa-
upload:before{content:"\F093"}.fa-lemon-o:before{content:"\F094"}.fa-
phone:before{content:"\F095"}.fa-square-o:before{content:"\F096"}.fa-bookmark-
o:before{content:"\F097"}.fa-phone-square:before{content:"\F098"}.fa-
twitter:before{content:"\F099"}.fa-facebook-f:before,.fa-facebook:before{content:"\F09A"}.fa-
github:before{content:"\F09B"}.fa-unlock:before{content:"\F09C"}.fa-credit-
card:before{content:"\F09D"}.fa-feed:before,.fa-rss:before{content:"\F09E"}.fa-hdd-
o:before{content:"\F0A0"}.fa-bullhorn:before{content:"\F0A1"}.fa-
bell:before{content:"\F0A3"}.fa-certificate:before{content:"\F0A3"}.fa-hand-o-
right:before{content:"\F0A4"}.fa-hand-o-left:before{content:"\F0A5"}.fa-hand-o-
up:before{content:"\F0A6"}.fa-hand-o-down:before{content:"\F0A7"}.fa-arrow-circle-
left:before{content:"\F0A8"}.fa-arrow-circle-right:before{content:"\F0A9"}.fa-arrow-circle-
up:before{content:"\F0AA"}.fa-arrow-circle-down:before{content:"\F0AB"}.fa-
globe:before{content:"\F0AC"}.fa-wrench:before{content:"\F0AD"}.fa-
tasks:before{content:"\F0AE"}.fa-filter:before{content:"\F0B0"}.fa-
briefcase:before{content:"\F0B1"}.fa-arrows-alt:before{content:"\F0B2"}.fa-group:before,.fa-
users:before{content:"\F0C0"}.fa-chain:before,.fa-link:before{content:"\F0C1"}.fa-
cloud:before{content:"\F0C2"}.fa-flask:before{content:"\F0C3"}.fa-cut:before,.fa-
scissors:before{content:"\F0C4"}.fa-copy:before,.fa-files-o:before{content:"\F0C5"}.fa-
paperclip:before{content:"\F0C6"}.fa-save:before,.fa-floppy-o:before{content:"\F0C7"}.fa-
square:before{content:"\F0C8"}.fa-navicon:before,.fa-reorder:before,.fa-
bars:before{content:"\F0C9"}.fa-list-ul:before{content:"\F0CA"}.fa-list-
ol:before{content:"\F0CB"}.fa-strikethrough:before{content:"\F0CC"}.fa-
underline:before{content:"\F0CD"}.fa-table:before{content:"\F0CE"}.fa-
magic:before{content:"\F0D0"}.fa-truck:before{content:"\F0D1"}.fa-
pinterest:before{content:"\F0D2"}.fa-pinterest-square:before{content:"\F0D3"}.fa-google-plus-
square:before{content:"\F0D4"}.fa-google-plus:before{content:"\F0D5"}.fa-
money:before{content:"\F0D6"}.fa-caret-down:before{content:"\F0D7"}.fa-caret-
up:before{content:"\F0D8"}.fa-caret-left:before{content:"\F0D9"}.fa-caret-
right:before{content:"\F0DA"}.fa-columns:before{content:"\F0DB"}.fa-unsorted:before,.fa-
sort:before{content:"\F0DC"}.fa-sort-down:before,.fa-sort-desc:before{content:"\F0DD"}.fa-sort-
up:before,.fa-sort-asc:before{content:"\F0DE"}.fa-envelope:before{content:"\F0E0"}.fa-
linkedin:before{content:"\F0E1"}.fa-rotate-left:before,.fa-undo:before{content:"\F0E2"}.fa-
legal:before,.fa-gavel:before{content:"\F0E3"}.fa-dashboard:before,.fa-
tachometer:before{content:"\F0E4"}.fa-comment-o:before{content:"\F0E5"}.fa-comments-
o:before{content:"\F0E6"}.fa-flash:before,.fa-bolt:before{content:"\F0E7"}.fa-
sitemap:before{content:"\F0E8"}.fa-umbrella:before{content:"\F0E9"}.fa-paste:before,.fa-
clipboard:before{content:"\F0EA"}.fa-lightbulb-o:before{content:"\F0EB"}.fa-
exchange:before{content:"\F0EC"}.fa-cloud-download:before{content:"\F0ED"}.fa-cloud-
upload:before{content:"\F0EE"}.fa-user-md:before{content:"\F0F0"}.fa-

```

```

stethoscope:before{content:"\\F0F1"}.fa-suitcase:before{content:"\\F0F2"}.fa-bell-
o:before{content:"\\F0A2"}.fa-coffee:before{content:"\\F0F4"}.fa-
cutlery:before{content:"\\F0F5"}.fa-file-text-o:before{content:"\\F0F6"}.fa-building-
o:before{content:"\\F0F7"}.fa-hospital-o:before{content:"\\F0F8"}.fa-
ambulance:before{content:"\\F0F9"}.fa-medkit:before{content:"\\F0FA"}.fa-fighter-
jet:before{content:"\\F0FB"}.fa-beer:before{content:"\\F0FC"}.fa-h-
square:before{content:"\\F0FD"}.fa-plus-square:before{content:"\\F0FE"}.fa-angle-double-
left:before{content:"\\F100"}.fa-angle-double-right:before{content:"\\F101"}.fa-angle-double-
up:before{content:"\\F102"}.fa-angle-double-down:before{content:"\\F103"}.fa-angle-
left:before{content:"\\F104"}.fa-angle-right:before{content:"\\F105"}.fa-angle-
up:before{content:"\\F106"}.fa-angle-down:before{content:"\\F107"}.fa-
desktop:before{content:"\\F108"}.fa-laptop:before{content:"\\F109"}.fa-
tablet:before{content:"\\F10A"}.fa-mobile-phone:before,.fa-mobile:before{content:"\\F10B"}.fa-
circle-o:before{content:"\\F10C"}.fa-quote-left:before{content:"\\F10D"}.fa-quote-
right:before{content:"\\F10E"}.fa-spinner:before{content:"\\F110"}.fa-
circle:before{content:"\\F111"}.fa-mail-reply:before,.fa-reply:before{content:"\\F112"}.fa-
github-alt:before{content:"\\F113"}.fa-folder-o:before{content:"\\F114"}.fa-folder-open-
o:before{content:"\\F115"}.fa-smile-o:before{content:"\\F118"}.fa-frown-
o:before{content:"\\F119"}.fa-meh-o:before{content:"\\F11A"}.fa-
gamepad:before{content:"\\F11B"}.fa-keyboard-o:before{content:"\\F11C"}.fa-flag-
o:before{content:"\\F11D"}.fa-flag-checkered:be

```

fore{content:"\\F11E"}.fa-terminal:before{content:"\\F120"}.fa-code:before{content:"\\F121"}.fa-mail-reply-
 all:before,.fa-reply-all:before{content:"\\F122"}.fa-star-half-empty:before,.fa-star-half-full:before,.fa-
 star-half-o:before{content:"\\F123"}.fa-location-arrow:before{content:"\\F124"}.fa-
 crop:before{content:"\\F125"}.fa-code-fork:before{content:"\\F126"}.fa-unlink:before,.fa-chain-
 broken:before{content:"\\F127"}.fa-question:before{content:"\\F128"}.fa-info:before{content:"\\F129"}.fa-
 exclamation:before{content:"\\F12A"}.fa-superscript:before{content:"\\F12B"}.fa-
 subscript:before{content:"\\F12C"}.fa-eraser:before{content:"\\F12D"}.fa-puzzle-
 piece:before{content:"\\F12E"}.fa-microphone:before{content:"\\F130"}.fa-microphone-
 slash:before{content:"\\F131"}.fa-shield:before{content:"\\F132"}.fa-calendar-o:before{content:"\\F133"}.fa-
 fire-extinguisher:before{content:"\\F134"}.fa-rocket:before{content:"\\F135"}.fa-
 maxcdn:before{content:"\\F136"}.fa-chevron-circle-left:before{content:"\\F137"}.fa-chevron-circle-
 right:before{content:"\\F138"}.fa-chevron-circle-up:before{content:"\\F139"}.fa-chevron-circle-
 down:before{content:"\\F13A"}.fa-html5:before{content:"\\F13B"}.fa-css3:before{content:"\\F13C"}.fa-
 anchor:before{content:"\\F13D"}.fa-unlock-alt:before{content:"\\F13E"}.fa-
 bullseye:before{content:"\\F140"}.fa-ellipsis-h:before{content:"\\F141"}.fa-ellipsis-
 v:before{content:"\\F142"}.fa-rss-square:before{content:"\\F143"}.fa-play-circle:before{content:"\\F144"}.fa-
 ticket:before{content:"\\F145"}.fa-minus-square:before{content:"\\F146"}.fa-minus-square-
 o:before{content:"\\F147"}.fa-level-up:before{content:"\\F148"}.fa-level-down:before{content:"\\F149"}.fa-
 check-square:before{content:"\\F14A"}.fa-pencil-square:before{content:"\\F14B"}.fa-external-link-
 square:before{content:"\\F14C"}.fa-share-square:before{content:"\\F14D"}.fa-
 compass:before{content:"\\F14E"}.fa-toggle-down:before,.fa-caret-square-o-down:before{content:"\\F150"}.fa-
 toggle-up:before,.fa-caret-square-o-up:before{content:"\\F151"}.fa-toggle-right:before,.fa-caret-square-o-
 right:before{content:"\\F152"}.fa-euro:before,.fa-eur:before{content:"\\F153"}.fa-
 gbp:before{content:"\\F154"}.fa-dollar:before,.fa-usd:before{content:"\\F155"}.fa-rupee:before,.fa-
 inr:before{content:"\\F156"}.fa-cny:before,.fa-rmb:before,.fa-yen:before,.fa-jpy:before{content:"\\F157"}.fa-
 ruble:before,.fa-rouble:before,.fa-rub:before{content:"\\F158"}.fa-won:before,.fa-
 krw:before{content:"\\F159"}.fa-bitcoin:before,.fa-btc:before{content:"\\F15A"}.fa-
 file:before{content:"\\F15B"}.fa-file-text:before{content:"\\F15C"}.fa-sort-alpha-
 asc:before{content:"\\F15D"}.fa-sort-alpha-desc:before{content:"\\F15E"}.fa-sort-amount-
 asc:before{content:"\\F160"}.fa-sort-amount-desc:before{content:"\\F161"}.fa-sort-numeric-
 asc:before{content:"\\F162"}.fa-sort-numeric-desc:before{content:"\\F163"}.fa-thumbs-
 up:before{content:"\\F164"}.fa-thumbs-down:before{content:"\\F165"}.fa-youtube-
 square:before{content:"\\F166"}.fa-youtube:before{content:"\\F167"}.fa-xing:before{content:"\\F168"}.fa-xing-
 square:before{content:"\\F169"}.fa-youtube-play:before{content:"\\F16A"}.fa-
 dropbox:before{content:"\\F16B"}.fa-stack-overflow:before{content:"\\F16C"}.fa-
 instagram:before{content:"\\F16D"}.fa-flickr:before{content:"\\F16E"}.fa-adn:before{content:"\\F170"}.fa-
 bitbucket:before{content:"\\F171"}.fa-bitbucket-square:before{content:"\\F172"}.fa-
 tumblr:before{content:"\\F173"}.fa-tumblr-square:before{content:"\\F174"}.fa-long-arrow-
 down:before{content:"\\F175"}.fa-long-arrow-up:before{content:"\\F176"}.fa-long-arrow-
 left:before{content:"\\F177"}.fa-long-arrow-right:before{content:"\\F178"}.fa-
 apple:before{content:"\\F179"}.fa-windows:before{content:"\\F17A"}.fa-android:before{content:"\\F17B"}.fa-
 linux:before{content:"\\F17C"}.fa-dribbble:before{content:"\\F17D"}.fa-skype:before{content:"\\F17E"}.fa-
 foursquare:before{content:"\\F180"}.fa-trello:before{content:"\\F181"}.fa-female:before{content:"\\F182"}.fa-
 male:before{content:"\\F183"}.fa-gittip:before,.fa-gratipay:before{content:"\\F184"}.fa-sun-
 o:before{content:"\\F185"}.fa-moon-o:before{content:"\\F186"}.fa-archive:before{content:"\\F187"}.fa-
 bug:before{content:"\\F188"}.fa-vk:before{content:"\\F189"}.fa-weibo:before{content:"\\F18A"}.fa-
 renren:before{content:"\\F18B"}.fa-pagelines:before{content:"\\F18C"}.fa-stack-
 exchange:before{content:"\\F18D"}.fa-arrow-circle-o-right:before{content:"\\F18E"}.fa-arrow-circle-o-
 left:before{content:"\\F190"}.fa-toggle-left:before,.fa-caret-square-o-left:before{content:"\\F191"}.fa-dot-
 circle-o:before{content:"\\F192"}.fa-wheelchair:before{content:"\\F193"}.fa-vimeo-
 square:before{content:"\\F194"}.fa-turkish-lira:before,.fa-try:before{content:"\\F195"}.fa-plus-square-
 o:before{content:"\\F196"}.fa-space-shuttle:before{content:"\\F197"}.fa-slack:before{content:"\\F198"}.fa-
 envelope-square:before{content:"\\F199"}.fa-wordpress:before{content:"\\F19A"}.fa-
 openid:before{content:"\\F19B"}.fa-institution:before,.fa-bank:before,.fa-
 university:before{content:"\\F19C"}.fa-mortar-board:before,.fa-graduation-cap:before{content:"\\F19D"}.fa-
 yahoo:before{content:"\\F19E"}.fa-google:before{content:"\\F1A0"}.fa-reddit:before{content:"\\F1A1"}.fa-
 reddit-square:before{content:"\\F1A2"}.fa-stumbleupon-circle:before{content:"\\F1A3"}.fa-
 stumbleupon:before{content:"\\F1A4"}.fa-delicious:before{content:"\\F1A5"}.fa-
 digg:before{content:"\\F1A6"}.fa-pied-piper-pp:before{content:"\\F1A7"}.fa-pied-piper-
 alt:before{content:"\\F1A8"}.fa-drupal:before{content:"\\F1A9"}.fa-joomla:before{content:"\\F1AA"}.fa-
 language:before{content:"\\F1AB"}.fa-fax:before{content:"\\F1AC"}.fa-building:before{content:"\\F1AD"}.fa-
 child:before{content:"\\F1AE"}.fa-paw:before{content:"\\F1B0"}.fa-spoon:before{content:"\\F1B1"}.fa-
 cube:before{content:"\\F1B2"}.fa-cubes:before{content:"\\F1B3"}.fa-behance:before{content:"\\F1B4"}.fa-
 behance-square:before{content:"\\F1B5"}.fa-steam:before{content:"\\F1B6"}.fa-steam-
 square:before{content:"\\F1B7"}.fa-recycle:before{content:"\\F1B8"}.fa-automobile:before,.fa-
 car:before{content:"\\F1B9"}.fa-cab:before,.fa-taxi:before{content:"\\F1BA"}.fa-
 tree:before{content:"\\F1BB"}.fa-spotify:before{content:"\\F1BC"}.fa-deviantart:before{content:"\\F1BD"}.fa-
 soundcloud:before{content:"\\F1BE"}.fa-database:before{content:"\\F1C0"}.fa-file-pdf-
 o:before{content:"\\F1C1"}.fa-file-word-o:before{content:"\\F1C2"}.fa-file-excel-
 o:before{content:"\\F1C3"}.fa-file-powerpoint-o:before{content:"\\F1C4"}.fa-file-photo-o:before,.fa-file-
 picture-o:before,.fa-file-image-o:before{content:"\\F1C5"}.fa-file-zip-o:before,.fa-file-archive-
 o:before{content:"\\F1C6"}.fa-file-sound-o:before,.fa-file-audio-o:before{content:"\\F1C7"}.fa-file-movie-
 o:before,.fa-file-video-o:before{content:"\\F1C8"}.fa-file-code-o:before{content:"\\F1C9"}.fa-
 vine:before{content:"\\F1CA"}.fa-codepen:before{content:"\\F1CB"}.fa-jsfiddle:before{content:"\\F1CC"}.fa-
 life-bouy:before,.fa-life-buoy:before,.fa-life-saver:before,.fa-support:before,.fa-life-

ring:before{content:"\\F1CD"}.fa-circle-o-notch:before{content:"\\F1CE"}.fa-ra:before,.fa-resistance:before,.fa-rebel:before{content:"\\F1D0"}.fa-ge:before,.fa-empire:before{content:"\\F1D1"}.fa-git-square:before{content:"\\F1D2"}.fa-git:before{content:"\\F1D3"}.fa-y-combinator-square:before,.fa-yc-square:before,.fa-hacker-news:before{content:"\\F1D4"}.fa-tencent-weibo:before{content:"\\F1D5"}.fa-qq:before{content:"\\F1D6"}.fa-wechat:before,.fa-weixin:before{content:"\\F1D7"}.fa-send:before,.fa-paper-plane:before{content:"\\F1D8"}.fa-send-o:before,.fa-paper-plane-o:before{content:"\\F1D9"}.fa-history:before{content:"\\F1DA"}.fa-circle-thin:before{content:"\\F1DB"}.fa-header:before{content:"\\F1DC"}.fa-paragraph:before{content:"\\F1DD"}.fa-sliders:before{content:"\\F1DE"}.fa-share-alt:before{content:"\\F1E0"}.fa-share-alt-square:before{content:"\\F1E1"}.fa-bomb:before{content:"\\F1E2"}.fa-soccer-ball-o:before,.fa-futbol-o:before{content:"\\F1E3"}.fa-tty:before{content:"\\F1E4"}.fa-binoculars:before{content:"\\F1E5"}.fa-plug:before{content:"\\F1E6"}.fa-slideshare:before{content:"\\F1E7"}.fa-twitch:before{content:"\\F1E8"}.fa-yelp:before{content:"\\F1E9"}.fa-newspaper-o:before{content:"\\F1EA"}.fa-wifi:before{content:"\\F1EB"}.fa-calculator:before{content:"\\F1EC"}.fa-paypal:before{content:"\\F1ED"}.fa-google-wallet:before{content:"\\F1EE"}.fa-cc-visa:before{content:"\\F1F0"}.fa-cc-mastercard:before{content:"\\F1F1"}.fa-cc-discover:before{content:"\\F1F2"}.fa-cc-amex:before{content:"\\F1F3"}.fa-cc-paypal:before{content:"\\F1F4"}.fa-cc-stripe:before{content:"\\F1F5"}.fa-bell-slash:before{content:"\\F1F6"}.fa-bell-slash-o:before{content:"\\F1F7"}.fa-trash:before{content:"\\F1F8"}.fa-copyright:before{content:"\\F1F9"}.fa-at:before{content:"\\F1FA"}.fa-eyedropper:before{content:"\\F1FB"}.fa-paint-brush:before{content:"\\F1FC"}.fa-birthday-cake:before{content:"\\F1FD"}.fa-area-chart:before{content:"\\F1FE"}.fa-pie-chart:before{content:"\\F200"}.fa-line-chart:before{content:"\\F201"}.fa-lastfm:before{content:"\\F202"}.fa-lastfm-square:before{content:"\\F203"}.fa-toggle-off:before{content:"\\F204"}.fa-toggle-on:before{content:"\\F205"}.fa-bicycle:before{content:"\\F206"}.fa-bus:before{content:"\\F207"}.fa-ioxhost:before{content:"\\F208"}.fa-angellist:before{content:"\\F209"}.fa-cc:before{content:"\\F20A"}.fa-shekel:before,.fa-sheqel:before,.fa-ils:before{content:"\\F20B"}.fa-meanpath:before{content:"\\F20C"}.fa-buysellads:before{content:"\\F20D"}.fa-connectdevelop:before{content:"\\F20E"}.fa-dashcube:before{content:"\\F210"}.fa-forumbee:before{content:"\\F211"}.fa-leanpub:before{content:"\\F212"}.fa-sellsy:before{content:"\\F213"}.fa-shirtsinbulk:before{content:"\\F214"}.fa-simplybuilt:before{content:"\\F215"}.fa-skyatlas:before{content:"\\F216"}.fa-cart-plus:before{content:"\\F217"}.fa-cart-arrow-down:before{content:"\\F218"}.fa-diamond:before{content:"\\F219"}.fa-ship:before{content:"\\F21A"}.fa-user-secret:before{content:"\\F21B"}.fa-motorcycle:before{content:"\\F21C"}.fa-street-view:before{content:"\\F21D"}.fa-heartbeat:before{content:"\\F21E"}.fa-venus:before{content:"\\F221"}.fa-mars:before{content:"\\F222"}.fa-mercury:before{content:"\\F223"}.fa-intersex:before,.fa-transgender:before{content:"\\F224"}.fa-transgender-alt:before{content:"\\F225"}.fa-venus-double:before{content:"\\F226"}.fa-mars-double:before{content:"\\F227"}.fa-venus-mars:before{content:"\\F228"}.fa-mars-stroke:before{content:"\\F229"}.fa-mars-stroke-v:before{content:"\\F22A"}.fa-mars-stroke-h:before{content:"\\F22B"}.fa-neuter:before{content:"\\F22C"}.fa-genderless:before{content:"\\F22D"}.fa-facebook-official:before{content:"\\F230"}.fa-pinterest-p:before{content:"\\F231"}.fa-whatsapp:before{content:"\\F232"}.fa-server:before{content:"\\F233"}.fa-user-plus:before{content:"\\F234"}.fa-user-times:before{content:"\\F235"}.fa-hotel:before,.fa-bed:before{content:"\\F236"}.fa-viacoin:before{content:"\\F237"}.fa-train:before{content:"\\F238"}.fa-subway:before{content:"\\F239"}.fa-medium:before{content:"\\F23A"}.fa-yc:before,.fa-y-combinator:before{content:"\\F23B"}.fa-optin-monster:before{content:"\\F23C"}.fa-opencart:before{content:"\\F23D"}.fa-expeditedssl:before{content:"\\F23E"}.fa-battery-4:before,.fa-battery:before,.fa-battery-full:before{content:"\\F240"}.fa-battery-3:before,.fa-battery-three-quarters:before{content:"\\F241"}.fa-battery-2:before,.fa-battery-half:before{content:"\\F242"}.fa-battery-1:before,.fa-battery-quarter:before{content:"\\F243"}.fa-battery-0:before,.fa-battery-empty:before{content:"\\F244"}.fa-mouse-pointer:before{content:"\\F245"}.fa-i-cursor:before{content:"\\F246"}.fa-object-group:before{content:"\\F247"}.fa-object-ungroup:before{content:"\\F248"}.fa-sticky-note:before{content:"\\F249"}.fa-sticky-note-o:before{content:"\\F24A"}.fa-cc-jcb:before{content:"\\F24B"}.fa-cc-diners-club:before{content:"\\F24C"}.fa-clone:before{content:"\\F24D"}.fa-balance-scale:before{content:"\\F24E"}.fa-hourglass-o:before{content:"\\F250"}.fa-hourglass-1:before,.fa-hourglass-start:before{content:"\\F251"}.fa-hourglass-2:before,.fa-hourglass-half:before{content:"\\F252"}.fa-hourglass-3:before,.fa-hourglass-end:before{content:"\\F253"}.fa-hourglass:before{content:"\\F254"}.fa-hand-rock-o:before,.fa-hand-rock-o:before{content:"\\F255"}.fa-hand-stop-o:before,.fa-hand-paper-o:before{content:"\\F256"}.fa-hand-scissors-o:before{content:"\\F257"}.fa-hand-lizard-o:before{content:"\\F258"}.fa-hand-spock-o:before{content:"\\F259"}.fa-hand-pointer-o:before{content:"\\F25A"}.fa-hand-peace-o:before{content:"\\F25B"}.fa-trademark:before{content:"\\F25C"}.fa-registered:before{content:"\\F25D"}.fa-creative-commons:before{content:"\\F25E"}.fa-gg:before{content:"\\F260"}.fa-gg-circle:before{content:"\\F261"}.fa-tripadvisor:before{content:"\\F262"}.fa-odnoklassniki:before{content:"\\F263"}.fa-odnoklassniki-square:before{content:"\\F264"}.fa-get-pocket:before{content:"\\F265"}.fa-wikipedia-w:before{content:"\\F266"}.fa-safari:before{content:"\\F267"}.fa-chrome:before{content:"\\F268"}.fa-firefox:before{content:"\\F269"}.fa-opera:before{content:"\\F26A"}.fa-internet-explorer:before{content:"\\F26B"}.fa-tv:before,.fa-television:before{content:"\\F26C"}.fa-contao:before{content:"\\F26D"}.fa-500px:before{content:"\\F26E"}.fa-amazon:before{content:"\\F270"}.fa-calendar-plus-o:before{content:"\\F271"}.fa-calendar-minus-o:before{content:"\\F272"}.fa-calendar-times-o:before{content:"\\F273"}.fa-calendar-check-o:before{content:"\\F274"}.fa-industry:before{content:"\\F275"}.fa-map-pin:before{content:"\\F276"}.fa-map-signs:before{content:"\\F277"}.fa-map-o:before{content:"\\F278"}.fa-map:before{content:"\\F279"}.fa-commenting:before{content:"\\F27A"}.fa-commenting-o:before{content:"\\F27B"}.fa-houzz:before{content:"\\F27C"}.fa-vimeo:before{content:"\\F27D"}.fa-black-tie:before{content:"\\F27E"}.fa-fonticons:before{content:"\\F280"}.fa-reddit-alien:before{content:"\\F281"}.fa-edge:before{content:"\\F282"}.fa-credit-card-alt:before{content:"\\F283"}.fa-codiepie:before{content:"\\F284"}.fa-modx:before{content:"\\F285"}.fa-fort-awesome:before{content:"\\F286"}.fa-usb:before{content:"\\F287"}.fa-product-hunt:before{content:"\\F288"}.fa-

```

mixcloud:before{content:"\F289"}.fa-scribd:before{content:"\F28A"}.fa-pause-
circle:before{content:"\F28B"}.fa-pause-circle-o:before{content:"\F28C"}.fa-stop-
circle:before{content:"\F28D"}.fa-stop-circle-o:before{content:"\F28E"}.fa-shopping-
bag:before{content:"\F290"}.fa-shopping-basket:before{content:"\F291"}.fa-
hashtag:before{content:"\F292"}.fa-bluetooth:before{content:"\F293"}.fa-bluetooth-
b:before{content:"\F294"}.fa-percent:before{content:"\F295"}.fa-gitlab:before{content:"\F296"}.fa-
wpbeginner:before{content:"\F297"}.fa-wpforms:before{content:"\F298"}.fa-
envira:before{content:"\F299"}.fa-universal-access:before{content:"\F29A"}.fa-wheelchair-
alt:before{content:"\F29B"}.fa-question-circle-o:before{content:"\F29C"}.fa-
blind:before{content:"\F29D"}.fa-audio-description:before{content:"\F29E"}.fa-volume-control-
phone:before{content:"\F2A0"}.fa-braille:before{content:"\F2A1"}.fa-assistive-listening-
systems:before{content:"\F2A2"}.fa-asl-interpreting:before,.fa-american-sign-language-
interpreting:before{content:"\F2A3"}.fa-deafness:before,.fa-hard-of-hearing:before,.fa-
deaf:before{content:"\F2A4"}.fa-glide:before{content:"\F2A5"}.fa-glide-g:before{content:"\F2A6"}.fa-
signing:before,.fa-sign-language:before{content:"\F2A7"}.fa-low-vision:before{content:"\F2A8"}.fa-
viadeo:before{content:"\F2A9"}.fa-viadeo-square:before{content:"\F2AA"}.fa-
snapchat:before{content:"\F2AB"}.fa-snapchat-ghost:before{content:"\F2AC"}.fa-snapchat-
square:before{content:"\F2AD"}.fa-pied-piper:before{content:"\F2AE"}.fa-first-
order:before{content:"\F2B0"}.fa-yaost:before{content:"\F2B1"}.fa-themeisle:before{content:"\F2B2"}.fa-
google-plus-circle:before,.fa-google-plus-official:before{content:"\F2B3"}.fa-fa:before,.fa-font-
awesome:before{content:"\F2B4"}.fa-handshake-o:before{content:"\F2B5"}.fa-envelope-
open:before{content:"\F2B6"}.fa-envelope-open-o:before{content:"\F2B7"}.fa-
linode:before{content:"\F2B8"}.fa-address-book:before{content:"\F2B9"}.fa-address-book-
o:before{content:"\F2BA"}.fa-vcard:before,.fa-address-card:before{content:"\F2BB"}.fa-vcard-o:before,.fa-
address-card-o:before{content:"\F2BC"}.fa-user-circle:before{content:"\F2BD"}.fa-user-circle-
o:before{content:"\F2BE"}.fa-user-o:before{content:"\F2C0"}.fa-id-badge:before{content:"\F2C1"}.fa-
drivers-license:before,.fa-id-card:before{content:"\F2C2"}.fa-drivers-license-o:before,.fa-id-card-
o:before{content:"\F2C3"}.fa-quora:before{content:"\F2C4"}.fa-free-code-camp:before{content:"\F2C5"}.fa-
telegram:before{content:"\F2C6"}.fa-thermometer-4:before,.fa-thermometer:before,.fa-thermometer-
full:before{content:"\F2C7"}.fa-thermometer-3:before,.fa-thermometer-three-
quarters:before{content:"\F2C8"}.fa-thermometer-2:before,.fa-thermometer-half:before{content:"\F2C9"}.fa-
thermometer-1:before,.fa-thermometer-quarter:before{content:"\F2CA"}.fa-thermometer-0:before,.fa-
thermometer-empty:before{content:"\F2CB"}.fa-shower:before{content:"\F2CC"}.fa-bathtub:before,.fa-
s15:before,.fa-bath:before{content:"\F2CD"}.fa-podcast:before{content:"\F2CE"}.fa-window-
maximize:before{content:"\F2D0"}.fa-window-minimize:before{content:"\F2D1"}.fa-window-
restore:before{content:"\F2D2"}.fa-times-rectangle:before,.fa-window-close:before{content:"\F2D3"}.fa-
times-rectangle-o:before,.fa-window-close-o:before{content:"\F2D4"}.fa-bandcamp:before{content:"\F2D5"}.fa-
grav:before{content:"\F2D6"}.fa-etsy:before{content:"\F2D7"}.fa-imdb:before{content:"\F2D8"}.fa-
ravelry:before{content:"\F2D9"}.fa-eercast:before{content:"\F2DA"}.fa-
microchip:before{content:"\F2DB"}.fa-snowflake-o:before{content:"\F2DC"}.fa-
superpowers:before{content:"\F2DD"}.fa-wpexplorer:before{content:"\F2DE"}.fa-
meetup:before{content:"\F2E0"}.sr-only{position:absolute;width:1px;height:1px;padding:0;margin:-
1px;overflow:hidden;clip:rect(0,0,0,0);border:0}.sr-only-focusable:active,.sr-only-
focusable:focus{position:static;width:auto;height:auto;margin:0;overflow:visible;clip:auto}\n',""}}),"/node_
modules/css-loader/lib/css-base.js":function(e,o){function t(e,o){var t=e[1]||"",n=e[3];if(!n)return
t;if(o&&"function"===typeof btoa){var a=r(n);return[t].concat(n.sources.map(function(e){return"/#
sourceURL="+n.sourceRoot+e+" */"})).concat([a]).join("\n")}return[t].join("\n")}function r(e){return"/#
sourceMappingURL=data:application/json;charset=utf-
8;base64,"+btoa(unescape(encodeURIComponent(JSON.stringify(e))))+" */"}e.exports=function(e){var o=[];return
o.toString=function(){return this.map(function(o){var r=t(o,e);return o[2]?"@media "+o[2]+"
{"+r+"}":r}).join("")},o.i=function(e,t){"string"===typeof e&&(e=[null,e,""]);for(var r=
{},n=0;n<this.length;n++){var a=this[n][0]
...
...
...

```

Individuazione di possibile pattern di divulgazione percorso server

Severità:	Informazioni
Punteggio CVSS:	0,0
URL:	https://tst-secure.sistemapiemonte.it/conam/scripts.bundle.js
Entità:	scripts.bundle.js (Page)
Rischio:	È possibile richiamare il percorso assoluto di installazione del server Web, che potrebbe essere utile ad un aggressore per sviluppare altri attacchi ed ottenere informazioni sulla struttura del file system dell'applicazione Web
Cause:	Non sono state installate le patch o gli hotfix più recenti per i prodotti di terze parti.
Fix:	Scaricare la patch di sicurezza pertinente per il server Web o l'applicazione Web.

Differenza:

Motivazione: La risposta contiene i percorsi assoluti e/o nomi file di file presenti sul server.

Richieste e risposte del test:

[illegible]

31/01/2020

[illegible]

[illegible]

Problema 1 di 1

Sommar

Riferimenti cookie (JavaScript) lato client

Severità:

Informazioni

Punteggio CVSS: 0,0

URL:

<https://tst-secure.sistemapiemonte.it/conam/vendor.bundle.js>

Entità:

webpackJsonp([4],{"/.node_modules/@angular/animations/esm5/animations.js":function(e,t,r){
use stric... (Page)

Rischio:

Lo scenario di ipotesi peggiore per questo attacco dipende dal contesto e dal ruolo dei cookie creati sul lato client

Cause:

I cookie vengono creati sul lato client

Fix:

Rimuovere la logica di business e di sicurezza dal lato client

Differenza:

Motivazione: AppScan ha trovato un riferimento a cookie nel JavaScript.

Richieste e risposte del test:

```
GET /conam/vendor.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://tst-secure.sistemapiemonte.it/conam/
Cookie: PORTALE=SISTEMAPIEMONTE; JSESSIONID=hvvgPO2LMEJkpkf4F6Xxt7Ro.jb6part219conam_tunode02;
XSRF-TOKEN=26224895282259130793306388255943471480; PORTALE=SISTEMAPIEMONTE;
__shibsession_spsliv1$ISP=_1043e858854a3265c6dd5340455b3634;
__utma=260743567.231398534.1579858881.1579858881.1579861575.2;
__utmz=260743567.1579858881.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: Keep-Alive
Host: tst-secure.sistemapiemonte.it
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
X-XSRF-TOKEN: 26224895282259130793306388255943471480
```

```
HTTP/1.1 200 OK
Last-Modified: Tue, 21 Jan 2020 13:43:02 GMT
Connection: Keep-Alive
Server: Apache/2.4.41 (Unix) OpenSSL/1.1.1d mod_fcgid/2.3.9 mod_jk/1.2.46 PHP/5.6.40
Access-Control-Allow-Origin: https://tst-screen-sistemapiemonte.isan.csi.it
Accept-Ranges: bytes
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 1146414
Keep-Alive: timeout=5, max=93
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0
ETag: W/"1146414-1579614182000"
Date: Mon, 27 Jan 2020 16:27:17 GMT
Expires: 0
Content-Type: text/javascript
```

```
webpackJsonp([4],{"/.node_modules/@angular/animations/esm5/animations.js":function(e,t,r){  
use strict";function n(e,t){return void 0===t&&(t=null),{type:2,steps:e,options:t}}function o(e)  
{return{type:6,styles:e,offset:null}}/**  
 * @license  
 * Copyright Google Inc. All Rights Reserved.
```

```

*
* Use of this source code is governed by an MIT-style license that can be
* found in the LICENSE file at https://angular.io/license
* @param {?} cb
* @return {?}
*/
function i(e){Promise.resolve(null).then(e)}r.d(t,"b",function(){return s}),r.d(t,"c",function(){
{return a}),r.d(t,"a",function(){return u}),r.d(t,"e",function(){return n}),r.d(t,"f",function(){
{return o}),r.d(t,"d",function(){return c}),r.d(t,"g",function(){return l}),r.d(t,"h",function(){
{return p}));/**
 * @license Angular v5.2.11
 * (c) 2010-2018 Google, Inc. https://angular.io/
 * License: MIT
 */
var s=function(){function e(){}return e()},{a=function(){function e(){}return e}
(),u="",c=function(){function e(){this._onDoneFns=[],this._onStartFns=[],this._onDestroyFns=
[],this._started=1,this._destroyed=!1,this._finished=1,this.parentPlayer=null,this.totalTime=0}
return e.prototype._onFinish=function(){this._finished|
(this._finished=!0,this._onDoneFns.forEach(function(e){return e()}),this._onDoneFns=
[]),e.prototype.onStart=function(e){this._onStartFns.push(e)},e.prototype.onDone=function(e)
{this._onDoneFns.push(e)},e.prototype.onDestroy=function(e)
{this._onDestroyFns.push(e)},e.prototype.hasStarted=function(){return
this._started},e.prototype.init=function(){},e.prototype.play=function(){this.hasStarted()||
(this._onStart(),this.triggerMicrotask()),this._started=!0},e.protot
...
...
...
et=function(e,t){return"window"===t?window:"document"===t?e:"body"===t?
e.body:null},t.prototype.getHistory=function(){return
window.history},t.prototype.getLocation=function(){return
window.location},t.prototype.getBaseHref=function(e){var t=i();return null===t?
null:s(t)},t.prototype.resetBaseElement=function(){W=null},t.prototype.getUserAgent=function()
{return window.navigator.userAgent},t.prototype.setData=function(e,t,r)
{this.setAttribute(e,"data-"+t,r)},t.prototype.getData=function(e,t){return
this.getAttribute(e,"data-"+t)},t.prototype.getComputedStyle=function(e){return
getComputedStyle(e)},t.prototype.supportsWebAnimation=function(){return"function"===typeof
Element.prototype.animate},t.prototype.performanceNow=function(){return
window.performance&&window.performance.now?window.performance.now():(new
Date).getTime()},t.prototype.supportsCookies=function()
{return!0},t.prototype.getCookie=function(e){return Object(N.m)
(document.cookie,e)},t.prototype.setCookie=function(e,t)
{document.cookie=e+encodeURIComponent(e)+"="+encodeURIComponent(t)},t)
(L,W=null,G=N.d,K=function(e){function t(t){var r=e.call(this)||this;return
r._doc=t,r._init(),r}return Object(R.b)(t,e),t.prototype._init=function()
{this.location=n().getLocation(),this._history=n().getHistory()},t.prototype.getBaseHrefFromDOM=f
unction(){return n().getBaseHref(this._doc)},t.prototype.onPopState=function(e)
{n().getGlobalEventTarget(this._doc,"window").addEventListener("popstate",e,!1)},t.prototype.onHa
shChange=function(e)
{n().getGlobalEventTarget(this._doc,"window").addEventListener("hashchange",e,!1)},Object.defineP
roperty(t.prototype,"pathname",{get:function(){return this.location.pathname},set:function(e)
{this.location.pathname=e},enumerable:!0,configurable:!0}),Object.defineProperty(t.prototype,"sea
rch",{get:function(){return
this.location.search},enumerable:!0,configurable:!0}),Object.defineProperty(t.prototype,"hash",
{get:function(){return this.location.hash},e
...
...
...

```

Dati di applicazione

URL visitati 21

[Sommar](#)

URL
https://tst-secure.sistemapiemonte.it/conam
https://tst-secure.sistemapiemonte.it/conam
https://tst-secure.sistemapiemonte.it/conam
https://tst-secure.sistemapiemonte.it/conam/restfacade/user/getProfilo
https://tst-secure.sistemapiemonte.it/conam/restfacade/user/localLogout
https://tst-secure.sistemapiemonte.it/conam/inline.bundle.js
https://tst-secure.sistemapiemonte.it/conam/polyfills.bundle.js
https://tst-secure.sistemapiemonte.it/conam/scripts.bundle.js
https://tst-secure.sistemapiemonte.it/conam/styles.bundle.js
https://tst-secure.sistemapiemonte.it/conam/vendor.bundle.js
https://tst-secure.sistemapiemonte.it/conam/main.bundle.js
https://tst-secure.sistemapiemonte.it/conam
https://tst-secure.sistemapiemonte.it/conam/
https://tst-secure.sistemapiemonte.it/conam/inline.bundle.js
https://tst-secure.sistemapiemonte.it/conam/polyfills.bundle.js
https://tst-secure.sistemapiemonte.it/conam/scripts.bundle.js
https://tst-secure.sistemapiemonte.it/conam/styles.bundle.js
https://tst-secure.sistemapiemonte.it/conam/scripts.bundle.js
https://tst-secure.sistemapiemonte.it/conam
https://tst-secure.sistemapiemonte.it/conam/
https://tst-secure.sistemapiemonte.it/conam

Parametri 0

[Sommar](#)

Nome	Valore	URL	Tipo
------	--------	-----	------